Unveiling robustness and heterogeneity through percolation triggered by random-link breakdown

Yilun Shang
Department of Mathematics, Tongji University, Shanghai 200092, China
(Received 15 February 2014; revised manuscript received 12 June 2014; published 29 September 2014)

It has been commonly recognized that heterogeneously connected networks are robust against random decays but vulnerable to malicious attacks. However, little is known about measures of heterogeneity geared towards robustness of complex networks. Here, we propose two types of percolation on general networks triggered by random-link errors, where occupied links support the nodes to be alive. Rich resilience behaviors are observed in terms of the percolation threshold and the (integrated) fraction of giant cluster. The discrepancy unraveled between the two models allows us to dynamically define compact measures that have acute discrimination in gauging network heterogeneity. The results provide a connection between network performance, structure, and dynamics.

DOI: 10.1103/PhysRevE.90.032820 PACS number(s): 89.75.Hc, 64.60.ah, 84.35.+i

Networks with complex topology epitomize many real-world systems, whose operation essentially relies on their robustness, i.e., the ability to maintain global interconnectivity tolerating node and link errors [1–3]. Studies show that a variety of natural and man-made networks have a heavy-tailed degree distribution (that is, the distribution, p_k, which governs the probability that a node will have k edges attached to it) following approximately a power law [4]. Such networks (called *scale-free* networks), at variance with homogeneous Erdős-Rényi (ER) networks, consist of a small number of highly connected nodes (*hubs*) and a huge number of low-degree nodes. A key observation is that such heterogeneously connected networks are highly robust against random errors but appear extremely fragile to deliberate attacks at hubs [5] or edges connecting hubs [6].

By means of percolation theory [7–11], these resilience properties have been confirmed extensively by examining, e.g., the critical percolation threshold and the size of the largest cluster. This raises a challenging inverse question: Could heterogeneity be measured via percolation processes from a robustness-centric view? Alternatively, how does one derive a compact heterogeneity measure from percolation and understand its consequences on network robustness? We will show in Appendix D that the branching factor, which is a classical measure for heterogeneity, has no implication for network robustness. Moreover, heterogeneity is intimately related to other crucial dynamical properties such as synchronization [12], congestion [13], and spreading [14]. Thus, it is highly desirable to "customize" heterogeneity for specific processes over the network.

In this article, to quantify and compare the heterogeneity of networks, we study two types of percolation, termed α and β models, which are induced by random-link failure. In response to the link failure, a node fails in α model when the loss of its neighboring links exceeds a prescribed quantile (signified by a fraction α), while it fails in β model when the loss is above a certain quantity (signified by an absolute number β). This is reminiscent of what goes on in the bootstrap percolation [15], where occupied nodes, rather than links, are used as the support to the nodes to be alive. The link-triggered cascading failures occur in many real systems. For example, the blackouts in power grids are often triggered by line faults, which cause power flow redistribution onto neighboring nodes, overburdening other generators and lines due to excessive load [16]. Such threshold exceedance can be delineated by α model [17,18] or β model [19] across specific applications depending on how the failure is related to the capacity of the node in question.

Our analysis reveals that although a scale-free network with a degree exponent of under 3 is robust in both α and β models in the sense that the critical removal fraction of links tends to 1, the difference of robustness between the two models, in terms of percolation threshold, fraction of giant cluster, robustness index [20], etc., is much more prominent as compared with ER networks. The discrepancy between scale-free and ER networks makes it possible to define heterogeneity measures based on the percolation processes, providing an intriguing tie between network robustness, heterogeneity, and percolation.

To be concrete, we consider networks generated using the configuration model [21,22] (a random graph with a given degree distribution p_k). Initially, we assume that each link is occupied (intact) with probability q. For α model, a node is occupied if at least α proportion of its attached links are occupied, where $\alpha \in [0,1]$. Similarly, for β model, a node of degree k is occupied if at least $\min\{k,\beta\}$ of its attached links are occupied, where β is a non-negative integer and min is the minimum operator. For simplicity, we assume that the removal of a link due to node failure does not trigger further node failure. Thus, our models correspond to the initial stages of a cascading failure (cf. Appendix A). This is common in networks with a fault detection (or localization) mechanism: An attacked node may send warning signals to nearby nodes preventing faulty behavior from spreading [23].

If $\alpha = 0$, α model reduces to the case of uniform bond percolation [7]. So does β model for $\beta = 0$. For $\alpha > 0$ (resp., $\beta \geqslant 1$), α model (resp., β model) becomes a nonindependent joint bond and site percolation, which is often difficult to tackle analytically [11]. By Δ we indicate the maximum degree of the network. Then, α model for $\alpha = 1$ is equivalent to β model for any $\beta \geqslant \Delta$. The two identifying extremes together with the revealing fact that the two models are equivalent for k-regular graphs under relation $\alpha = \min\{k,\beta\}/k$ will later give us a good clue for the development of heterogeneity measures.

To proceed, we adopt the probability generating function method [22]. For α model, a node of degree k is occupied with probability $\sum_{i=0}^{(1-\alpha)k}\binom{k}{i}(1-q)^i q^{k-i}$ via binomial

distribution [24]. Thus, the probability generating function for occupied node degree distribution [7] is given by

$$F_0^{(\alpha)}(x) = \sum_{k=0}^{\infty} \sum_{i=0}^{(1-\alpha)k} p_k \binom{k}{i} (1-q)^i q^{k-i} x^k. \quad (1)$$

For β model, likewise we have

$$F_0^{(\beta)}(x) = \sum_{k=0}^{\infty} \sum_{i=0}^{k-\min\{k,\beta\}} p_k \binom{k}{i} (1-q)^i q^{k-i} x^k. \quad (2)$$

Suppose that we follow a randomly chosen edge, and the node reached is denoted by v_0. For α model, the probability that v_0 and the selected edge are both occupied is $q[\sum_{i=0}^{(1-\alpha)k} \binom{k-1}{i}(1-q)^i q^{k-1-i}]$, where the first term q is due to the occupation of the edge and the second term is due to the occupation of v_0 given it has degree k and the incoming edge is occupied [25]. Therefore, the distribution of the number of edges leading out of v_0 (called the excess degree distribution [22]) is generated by

$$F_1^{(\alpha)}(x) = \frac{\sum_{k=1}^{\infty} \sum_{i=0}^{(1-\alpha)k} k p_k \binom{k-1}{i} (1-q)^i q^{k-i} x^{k-1}}{\langle k \rangle}, \quad (3)$$

where $\langle k \rangle = \sum_{k=0}^{\infty} k p_k$ is the average degree. Similarly, for the β model,

$$F_1^{(\beta)}(x) = \frac{\sum_{k=1}^{\infty} \sum_{i=0}^{k-\min\{k,\beta\}} k p_k \binom{k-1}{i} (1-q)^i q^{k-i} x^{k-1}}{\langle k \rangle}. \quad (4)$$

Noting that $F_1(x) \neq F_0'(x)/\langle k \rangle$ [26], our percolation models are different from ordinary joint bond and site percolation [7].

Let $H_1^{(\alpha)}(x)$ and $H_1^{(\beta)}(x)$ be the generating functions, in α and β models, respectively, for the distribution of the sizes of percolation clusters that are reached by choosing a random edge and following it to its end, say, v_0. As ordinary percolation, a percolation cluster here is defined as the set of occupied nodes which are mutually reachable along occupied edges. Therefore, $H_1(x)$ satisfies the self-consistent condition

$$H_1(x) = 1 - F_1(1) + x F_1[H_1(x)], \quad (5)$$

where $1 - F_1(1)$ is the probability that the cluster contains zero nodes (either v_0 is unoccupied, or the selected edge is deleted), and the term $x F_1[H_1(x)]$ takes into account an occupied v_0 with k other edges leading out of it, distributed according to $F_1(x)$ [7]. The probability distributions of the size of the percolation cluster to which a randomly chosen node belongs are analogously generated by $H_0^{(\alpha)}(x)$ and $H_0^{(\beta)}(x)$, respectively, in the two models, where

$$H_0(x) = 1 - F_0(1) + x F_0[H_1(x)]. \quad (6)$$

One can check that (6) reproduces [7, Eq. (7)] (the uniform bond percolation case) when $\alpha = 0$ or $\beta = 0$.

With relations (5) and (6) in hand, the mean size of cluster to which a randomly chosen node belongs, in the absence of giant clusters, can be calculated as $\langle s \rangle = H_0'(1) = F_0(1) + F_0'(1)F_1(1)[1 - F_1'(1)]^{-1}$. This expression diverges at $F_1'(1) = 1$, which corresponds to the critical percolation threshold q_c where a giant cluster first emerges, yielding

$$\frac{\sum_{k=2}^{\infty} k(k-1) p_k \sum_{i=0}^{(1-\alpha)k} \binom{k-1}{i} \left(1 - q_c^{(\alpha)}\right)^i \left(q_c^{(\alpha)}\right)^{k-i}}{\langle k \rangle} = 1 \quad (7)$$

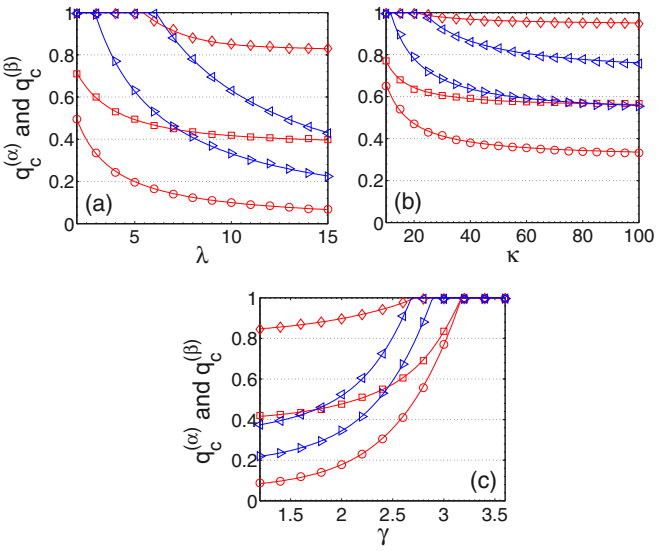

FIG. 1. (Color online) Percolation thresholds $q_c^{(\alpha)}$ and $q_c^{(\beta)}$ for networks of 10^6 nodes from numerical simulations with $\alpha = 0$ or $\beta = 0$ (circles), $\alpha = 0.5$ (squares), $\alpha = 0.9$ (diamonds), $\beta = 5$ (right triangles), $\beta = 10$ (left triangles), and exact solutions (solid lines): (a) for ER graphs with $\langle k \rangle = \lambda$, (b) for scale-free networks with degree exponent $\gamma = 2.5$ and exponential cutoff κ, and (c) for scale-free networks with $\kappa = 60$ and degree exponent γ.

for α model, and respectively,

$$\frac{\sum_{k=2}^{\infty} k(k-1) p_k \sum_{i=0}^{k-\min\{k,\beta\}} \binom{k-1}{i} \left(1 - q_c^{(\beta)}\right)^i \left(q_c^{(\beta)}\right)^{k-i}}{\langle k \rangle} = 1 \quad (8)$$

for β model. For a network with pure power-law distribution $p_k \sim k^{-\gamma}$, as shown in the Appendix C, $q_c^{(\alpha)} \to 0$ for any $\alpha \in [0,1]$ when $1 \leqslant \gamma < 3$. This suggests that such a network remains robust in α model—encompassing a special case of $\alpha = 0$, which recovers the "robust against random decay" paradigm of Cohen *et al.* [8,27]. Analogously, we have $q_c^{(\beta)} \to 0$ for any β when $1 \leqslant \gamma < 3$.

In Fig. 1 we show the critical occupation probabilities $q_c^{(\alpha)}$ and $q_c^{(\beta)}$ for different values of α and β in ER graphs with a Poisson degree distribution $p_k = e^{-\lambda}\lambda^k/k!$ $(k \geqslant 0)$ and scale-free graphs with a truncated power-law distribution $p_k \sim k^{-\gamma} e^{-k/\kappa}$ $(k \geqslant 1)$, featuring various real-life networks [4,22]. Throughout the article, plots for α and β models are shown in red and blue, respectively. The algorithm is given in Appendix B.

The agreement between the simulations and theory is excellent. For any given λ, κ, or γ, the models undergo a smooth transition from mild random breakdown with small $q_c^{(\alpha)}, q_c^{(\beta)}$ (corresponding to small α, β) to extremely harmful degree-dependent cascading failure with large $q_c^{(\alpha)}, q_c^{(\beta)}$ (corresponding to large α, β). Moreover, $q_c^{(\alpha)} \sim 1$ and $q_c^{(\beta)} \sim 1$ for small λ [in ER graphs; see Fig. 1(a)] and for small κ or large γ [in scale-free networks; see Figs. 1(b) and 1(c)] when α approaches 1 and β approaches Δ, respectively [28]. However, when it comes to a scale-free network without cutoff ($\kappa \to \infty$ and $\gamma < 3$), as we mentioned above, $q_c^{(\alpha)}, q_c^{(\beta)} \sim 0$ even for

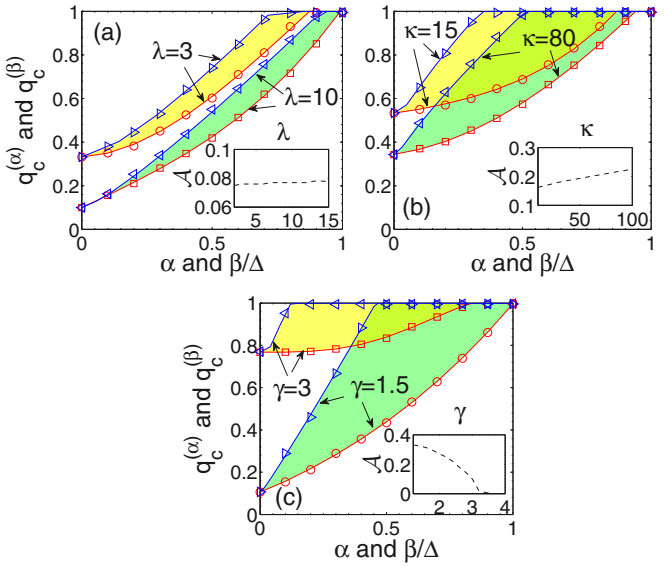

FIG. 2. (Color online) Percolation thresholds $q_c^{(\alpha)}$ (squares and circles) and $q_c^{(\beta)}$ (left and right triangles) as functions of α and β/Δ, respectively, for the same systems used in Fig. 1: (a) ER graphs with $\lambda = 3,10$; (b) scale-free networks with $\kappa = 15,80$ and $\gamma = 2.5$; (c) scale-free networks with $\gamma = 1.5,3$ and $\kappa = 60$. Points are the simulation results and lines are the exact solutions. The insets show the dependence of the heterogeneity index $\mathcal{A}$ on (a) λ, (b) κ given $\gamma = 2.5$, and (c) γ given $\kappa = 60$.

large α,β. This highlights the importance of identifying correct degree distribution in realistic networks [29], which could markedly affect the structural robustness.

The difference between α and β models is better appreciated when turning to the results reported in Fig. 2. With α and β/Δ sharing the same domain $[0,1]$ [30], the two curves $q_c^{(\alpha)}$ and $q_c^{(\beta)}$ form a closed contour for a given network as expected from model construction. When $\beta = \alpha\Delta$, a node with degree $k < \Delta$ in a network under β model is more likely to be deleted than that in a network under α model (This can be discerned from Fig. 2, where the curve $q_c^{(\beta)}$ is always above the curve $q_c^{(\alpha)}$). Thus, we propose a network heterogeneity measure based on percolation threshold as [31]

$$\mathcal{A} = \int_0^1 \left(q_c^{(\beta)}(\alpha\Delta) - q_c^{(\alpha)}(\alpha)\right) d\alpha, \tag{9}$$

which is equivalent to the area within a contour as shown in Fig. 2 (yellow and green areas), and gives the value 0 for a regular graph. A heterogeneous network generally corresponds to a large $\mathcal{A}$ value—the insets of Fig. 2 reveal that ER graphs keep a low $\mathcal{A}$ value about 0.075; in scale-free networks with $\gamma = 2.5$, an increase in the cutoff κ (meaning a longer tail in degree distribution) systematically yields an increase in $\mathcal{A}$ [cf. Fig. 3(d) inset]; given cutoff $\kappa = 60$, $\mathcal{A}$ decreases from above 0.3 to vanishing values with the increase of γ, leading to a more homogeneous degree distribution.

Next, we investigate the fraction of giant cluster, which will help us better understand the fragmentation process on the network. Denote by $S^{(\alpha)}$ and $S^{(\beta)}$ the fraction of nodes in the giant cluster in α and β models, respectively. Since $H_0(x)$ generates the size distribution of nongiant clusters, we obtain

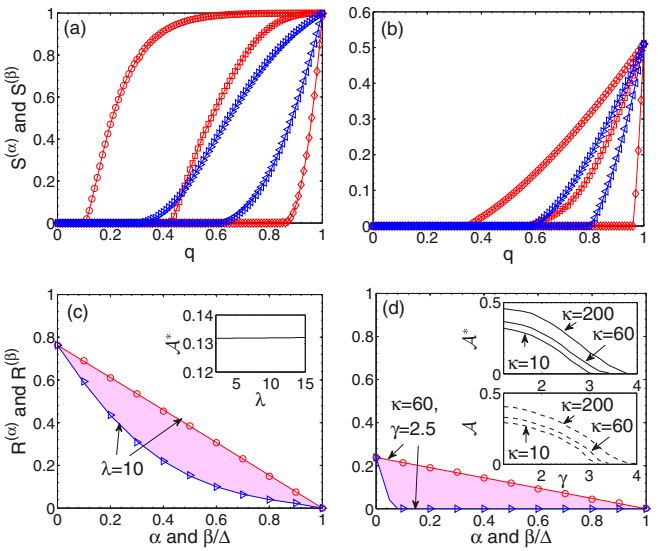

FIG. 3. (Color online) Top row [(a) and (b)]: fractions of giant clusters $S^{(\alpha)}$ and $S^{(\beta)}$ as functions of q for $\alpha = 0$ or $\beta = 0$ (circles), $\alpha = 0.5$ (squares), $\alpha = 0.9$ (diamonds), $\beta = 5$ (right triangles), $\beta = 10$ (left triangles). Bottom row [(c) and (d)]: robustness indices $R^{(\alpha)}$ (circles) and $R^{(\beta)}$ (right triangles) as functions of α and β/Δ, respectively. Left column [(a) and (c)] is for ER graphs with $\lambda = 10$. Right column [(b) and (d)] is for scale-free networks with $\kappa = 60$ and $\gamma = 2.5$. The insets show the dependence of the heterogeneity indices (c) $\mathcal{A}^*$ on λ, and (d) $\mathcal{A}^*$ and $\mathcal{A}$ on κ and γ. The same systems are used as in Fig. 1, points are the simulation results, and lines are the exact solutions.

$H_0(1) = 1 - S$ [22]. Based on (5) and (6),

$$S = 1 - H_0(1) = F_0(1) - F_0(u), \tag{10}$$

where $u = H_1(1)$ is the smallest non-negative solution of the self-consistency equation $u = 1 - F_1(1) - F_1(u)$. The normalized mean size of nongiant clusters becomes $\langle s\rangle = H_0'(1)/H_0(1) = \{F_0(u)[1 - F_1'(u)] + F_0'(u)F_1(u)\}(1 - S)^{-1}[1 - F_1'(u)]^{-1}$ with a special case of $S = 0$ and $u = 1$, as obtained above, corresponding to the regime before the formation of a giant cluster.

A novel measure is recently put forward by Schneider *et al.* [20,32] to quantify network robustness under malicious attacks. It is regarded to be more reflective of the entire fragmentation process than the critical threshold q_c. Following their work, we here propose a robustness measure based on our models as (cf. Appendix E)

$$R = \frac{1}{E}\sum_{q=1/E}^{1} S(q) \sim \int_0^1 S(q)dq, \tag{11}$$

where E is the total number of edges and $S(q) = S$ is given by (10). A second heterogeneity measure in analogy to (9) is defined as

$$\mathcal{A}^* = \int_0^1 [R^{(\alpha)}(\alpha) - R^{(\beta)}(\alpha\Delta)]d\alpha, \tag{12}$$

where $R^{(\alpha)}(\alpha) = R^{(\alpha)}$ and $R^{(\beta)}(\beta) = R^{(\beta)}$ are the measures defined in (11) taking α and β models, respectively, into account.

Figure 3 displays the variations of the fraction of giant cluster with the occupation probability q, and the integrated changes gauged by the robustness and heterogeneity measures. The results gathered in Fig. 3 allow us to draw several interesting conclusions. First, the simulated results agree with their analytical counterparts. The phase transition points at $S^{(\alpha)} \sim 0$ and $S^{(\beta)} \sim 0$, as expected, coincide with the critical probabilities $q_c^{(\alpha)}$ and $q_c^{(\beta)}$ in Fig. 1, respectively. Compared to bootstrap percolation, the continuous transition found here is nontrivial because it is an outcome of two competing factors—more links but less nodes are deleted (cf. Appendix A).

Second, there is a pronounced difference on the convexity of S curves between ER graphs and scale-free networks when α and β are small. This phenomenon is rooted in the fact that low-degree nodes are much more likely to be deleted for small α and β. When q is large, ER networks experience fairly mild error due to its homogeneity (most nodes have degrees close to $\langle k \rangle$), suggesting a sigmoidal variation of S with respect to q [Fig. 3(a)]; however, in scale-free networks, the deletion of low-degree nodes constantly depreciates the hubs breaking the giant cluster apart, which explains the considerable decrease of S [Fig. 3(b)]. For large α and β, S for both ER and scale-free networks exhibits a rapid drop, even at high level of q because of the serious cascading effect.

Third, although the change of robustness index R with respect to α and β for ER graphs [e.g., from nearly 0.8 to 0; see Fig. 3(c)] is typically more pronounced than that for scale-free networks [e.g., from nearly 0.2 to 0; see Fig. 3(d)], we find a quite different story in terms of $\mathcal{A}^*$, the integrated difference between $R^{(\alpha)}$ and $R^{(\beta)}$ (pink areas in Fig. 3): ER graphs maintain a relatively low $\mathcal{A}^*$ value of about 0.132 (the nondependence on λ probably roots in their nearly regular degrees: the change of density contributes equivalently to R in α and β models.), while scale-free networks generally possess higher $\mathcal{A}^*$—which decreases as γ increases and increases as κ grows—in analogy to $\mathcal{A}$. For example, a scale-free network with $\gamma = 2$ and $\kappa = 60$ yields $\mathcal{A}^* \approx 0.28$, more than double that of an ER graph. It is worth mentioning that the curve $R^{(\alpha)}$ is higher than $R^{(\beta)}$ [see Figs. 3(c) and 3(d)] because a node with degree $k < \Delta$ in β model is more likely to be deleted than that in α model when $\beta = \alpha\Delta$. Such different sensitivity to degree distribution for α and β models offers a unique insight on how heterogeneous the network is overall—granting a regular network $\mathcal{A}^* = \mathcal{A} = 0$.

In summary, we presented a way of understanding the role of heterogeneity in a complex network and the consequences on its robustness. Two bootstraplike models were introduced and solved analytically with generating functions. A wealth of robustness behaviors of ER and scale-free networks under failures triggered by random-link error are shown. Furthermore, two measures for heterogeneity were introduced with implications on network robustness. The modeling approach also offers us the possibility of a quantitative study of the heterogeneity of arbitrary networks, predicting the resilience of real systems. To further assess heterogeneity in some more universal way than via the degree distribution, application of our methods to empirical and real networks (probably with varied structural features) would be helpful.

APPENDIX A: COMPARISON BETWEEN α, β MODELS AND BOOTSTRAP PERCOLATION

There are two main differences between our model and the bootstrap percolation [15]. First, unlike the bootstrap percolation, we use occupied links, rather than nodes, as the support to the nodes to be alive. In bootstrap percolation, all links are intact. Second, we do not consider subsequent failures of nodes caused by node failure. The bootstrap percolation is an incremental process; nodes are deleted iteratively.

If we consider subsequent node failures in our model, it becomes analogous to the bootstrap percolation (both are incremental processes), and what is more, additional links are deleted in our model (note that no links are deleted in bootstrap percolation). Therefore, the "attack" would become more harmful than the bootstrap percolation; we are then in a good position to infer that an avalanche should happen. Moreover, it is reasonable to anticipate a first order transition, as is the case in [15,33,34], due to the analogy of bootstrap percolation. Of course, this last point is worth a more thorough investigation and is out of the scope of the present paper.

APPENDIX B: ALGORITHM IN SIMULATIONS

The network model used here is the configuration model, which can be generated using the software NETWORKX (see http://networkx.github.io/). For example, the following code is used to generate a scale-free graph with $\gamma = 2$, $\kappa = 20$, and $N = 10^6$:

```
>>>import networkx as nx
>>>N = 100 000 0
>>>a = [k**(-2)*2.718 28**(-k/20) for k in range(N)[1:N]]
>>>z = nx.utils.discrete_sequence(N,distribution = a)
>>>G = nx.configuration_model(z)
>>>import matplotlib.pyplot as plt
>>>nx.draw(G) >>> plt.show()
```

The algorithm used in generating Fig. 1 can be described as follows. We begin with $q = 1$ and delete each link in a network independently with probability $1 - q$. All nodes remain occupied (i.e., intact) so far. For each node (say, its initial degree is k) of the network, we check whether its current degree is bigger than $(1 - \alpha)k$ in α model, or $k - \min\{k, \beta\}$ in β model. If so, we do nothing; otherwise, we mark the node. After checking all nodes, we delete those having a mark. We then calculate the fraction S of the giant cluster. We decrease q by 10^{-4} and repeat the above process until $S < 10^{-3}$. The final output is q_c.

APPENDIX C: PROOF FOR $q_c^{(\alpha)} \to 0$ IN NETWORKS WITH DEGREE DISTRIBUTION $p_k \sim k^{-\gamma}$

We rewrite Eq. (7) as

$$q_c^{(\alpha)} \frac{\sum_{k=2}^{\infty} k(k-1)p_k \sum_{i=0}^{(1-\alpha)k} \binom{k-1}{i} \left(1 - q_c^{(\alpha)}\right)^i \left(q_c^{(\alpha)}\right)^{k-1-i}}{\langle k \rangle} = 1 \tag{C1}$$

by extracting one factor $q_c^{(\alpha)}$. For any $\alpha \in [0,1]$, $q_c^{(\alpha)} > 0$, and $k \geqslant 2$, there exists some constant $A = A(\alpha) > 0$ such that

$$0 < A \leqslant \sum_{i=0}^{(1-\alpha)k} \binom{k-1}{i} \left(1 - q_c^{(\alpha)}\right)^i \left(q_c^{(\alpha)}\right)^{k-1-i} \leqslant 1.$$

Hence, using (C1) we obtain

$$q_c^{(\alpha)} A \frac{\langle k^2 \rangle - \langle k \rangle}{\langle k \rangle} = q_c^{(\alpha)} \frac{A \sum_{k=2}^{\infty} k(k-1) p_k}{\langle k \rangle} \leqslant 1.$$

For a network with pure power-law distribution $p_k \sim k^{-\gamma}$, we know that $\langle k^2 \rangle / \langle k \rangle \to \infty$ for $1 \leqslant \gamma < 3$ [22]. Therefore, we are led to the conclusion that $q_c^{(\alpha)} \to 0$. The result $q_c^{(\beta)} \to 0$ can be shown in parallel.

APPENDIX D: INAPPROPRIATENESS OF BRANCHING FACTOR

In this section, we explain why the classical branching factor is not appropriate when robustness is taken into account.

As mentioned above, for a "pure" scale-free network with exponent $1 \leqslant \gamma < 3$, the branching factor $\langle k^2 \rangle / \langle k \rangle - 1$ diverges. For an ER graph with average degree $\langle k \rangle = \lambda$, the branching factor equals λ, which can be made arbitrarily large (i.e., a very dense graph) for an infinite graph. For finite-size systems, the branching factors for both types of networks can also be made very close to each other. In other words, the branching factor assimilates a scale-free network with $1 \leqslant \gamma < 3$ to a dense ER graph. However, as seen in this work and many others, ER graphs (dense or sparse) have distinct robustness behaviors from scale-free networks. Hence, the branching factor does not have correct implication for network robustness.

For similar reasons, other traditional measures such as the variance of the degree and the difference of the spectral radius with the mean degree do not have appropriate robustness implications either.

APPENDIX E: USEFULNESS OF ROBUSTNESS INDEX *R*

The measure R was first developed in [20] to deal with targeted attacks. Since then it has been applied and extended in several interesting cases in network science. It is defined as [20]

$$R = \frac{1}{N} \sum_{Q=1}^{N} S(Q),$$

where N is the number of nodes and $S(Q)$ is the fraction of nodes in the largest connected cluster after removing $Q = qN$ nodes. Hence, $R = 1/N$ for star networks and $R = 0.5$ for fully connected networks. For random node percolation $R \approx 0.5$ for star and fully connected networks. However, for random-link percolation, the damage is mild. Thus, R modified as in (11) can be above the expected values of node percolation. This agrees with the observation in Fig. 3(c).

On the other hand, since R is a compact measure which essentially integrates S over q [see (11)], it is more reflective of the whole or average robustness of the network. The measure is also very convenient since for each network we have a number R as compared to a "cumbersome" curve $S(q)$. With this measure, it is easy to understand our heterogeneity measure $\mathcal{A}^*$ that is more appropriate for this process than the branching factor.

According to the above comments, the heterogeneity measure $\mathcal{A}^*$ tends to be more comprehensive but requires even more calculations, as compared to $\mathcal{A}$. Therefore, when it comes to characterizing empirical large-scale networks, the measure $\mathcal{A}$ might be more appealing.

[1] R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002).

[2] R. Cohen and S. Havlin, *Complex Networks: Structure, Robustness and Function* (Cambridge University Press, Cambridge, 2010).

[3] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Phys. Rep. **424**, 175 (2006).

[4] G. Caldarelli, *Scale-Free Networks: Complex Webs in Nature and Technology* (Oxford University Press, New York, 2007).

[5] R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **406**, 378 (2000).

[6] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Phys. Rev. E **65**, 056109 (2002).

[7] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).

[8] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).

[9] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).

[10] Y. Chen, G. Paul, R. Cohen, S. Havlin, S. P. Borgatti, F. Liljeros, and H. E. Stanley, Phys. Rev. E **75**, 046107 (2007).

[11] Y. Shang, Phys. Rev. E **89**, 012813 (2014).

[12] N. Masuda, N. Gibert, and S. Redner, Phys. Rev. E **82**, 010103 (2010).

[13] W.-X. Wang, B.-H. Wang, C.-Y. Yin, Y.-B. Xie, and T. Zhou, Phys. Rev. E **73**, 026111 (2006).

[14] M. Boguñá, C. Castellano, and R. Pastor-Satorras, Phys. Rev. Lett. **111**, 068701 (2013).

[15] G. J. Baxter, S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Phys. Rev. E **82**, 011103 (2010).

[16] Other examples include large-scale bankruptcy owing to capital chain ruptures during economical recession, and metabolites malfunction caused by initial link shocks in metabolic networks [35].

[17] A. E. Motter and Y.-C. Lai, Phys. Rev. E **66**, 065102 (2002).

[18] P. Crucitti, V. Latora, and M. Marchiori, Phys. Rev. E **69**, 045104 (2004).

[19] V. Kishore, M. S. Santhanam, and R. E. Amritkar, Phys. Rev. Lett. **106**, 188701 (2011).

[20] C. M. Schneider, A. A. Moreira, J. S. Andrade, Jr., S. Havlin, and H. J. Herrmann, Proc. Natl. Acad. Sci. U.S.A. **108**, 3838 (2011).

[21] M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. E **64**, 026118 (2001).

[22] M. E. J. Newman, *Networks: An Introduction* (Oxford University Press, New York, 2010).

[23] M. Médard and S. S. Lumetta, in *Encyclopedia of Telecommunications*, edited by J. G. Proakis (Wiley, New York, 2003).

[24] Throughout the article, we omit the rounding symbols for ease of presentation. Also, the convention $0^0 = 1$ is valued.

[25] Note that $\binom{k}{i} = 0$ if $i > k$.

[26] To be succinct, we suppress the superscipts (α) and (β) whenever the expression concerned holds, respectively, for both models.

[27] R. Cohen, S. Havlin, and D. ben-Avraham, in *Handbook of Graphs and Networks: From the Genome to the Internet*, edited by S. Bornholdt and H. G. Schuster (Wiley-VCH, Berlin, 2003), pp. 85–110.

[28] This phenomenon is qualitatively consistent with that reported in [36]—networks with sparse (i.e., small λ) or homogeneous (i.e., small κ or large γ) degree distributions are remarkably more vulnerable to global cascades.

[29] M. P. H. Stumpf, C. Wiuf, and R. M. May, Proc. Natl. Acad. Sci. U.S.A. **102**, 4221 (2005).

[30] For analytical results, Δ is taken as the smallest degree k such that $q_c^{(\beta)}$ becomes steady.

[31] By notation, we define $q_c^{(\alpha)}(\alpha) = q_c^{(\alpha)}$ and $q_c^{(\beta)}(\beta) = q_c^{(\beta)}$. The robustness envelope [37] is similar in spirit since contour representation is employed.

[32] C. M. Schneider, N. Yazdani, N. A. M. Araújo, S. Havlin, and H. J. Herrmann, Sci. Rep. **3**, 1969 (2013).

[33] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Nature (London) **464**, 1025 (2010).

[34] W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin, Phys. Rev. Lett. **108**, 228702 (2012).

[35] A. G. Smart, L. A. N. Amaral, and J. M. Ottino, Proc. Natl. Acad. Sci. U.S.A. **105**, 13223 (2008).

[36] D. J. Watts, Proc. Natl. Acad. Sci. U.S.A. **99**, 5766 (2002).

[37] S. Trajanovski, J. Martín-Hernández, W. Winterbach, and P. V. Mieghem, J. Complex Networks **1**, 44 (2013).