Impact of self-healing capability on network robustness

Yilun Shang

Department of Mathematics, Tongji University, 200092 Shanghai, China
(Received 10 January 2015; published 16 April 2015)

A wide spectrum of real-life systems ranging from neurons to botnets display spontaneous recovery ability. Using the generating function formalism applied to static uncorrelated random networks with arbitrary degree distributions, the microscopic mechanism underlying the depreciation-recovery process is characterized and the effect of varying self-healing capability on network robustness is revealed. It is found that the self-healing capability of nodes has a profound impact on the phase transition in the emergence of percolating clusters, and that salient difference exists in upholding network integrity under random failures and intentional attacks. The results provide a theoretical framework for quantitatively understanding the self-healing phenomenon in varied complex systems.

I. INTRODUCTION

The robustness against random and systemic failures is crucial for the stable operation and high performance of various kinds of social, technological, and biological networks [1,2]. In terms of degree distribution, complex networks can be classified into heterogeneous networks (such as scale-free networks [3] with a power-law degree distribution) and homogeneous networks (such as random graphs [4] and small-world models [5] with a Poisson degree distribution). It has been well demonstrated [6–9] that heterogeneous networks are highly robust against random failures but appear extremely fragile to attacks targeted at highly connected nodes, i.e., hubs.

Although the topological attribution, e.g., degree distribution, to network robustness has been intensively studied in the past decade, the influence of self-healing of nodes is much overlooked despite its relevance in many real-life networked systems [10]. Examples are polymer networks where new polymeric compounds in materials can be self-repaired bonding crack faces due to microencapsulated healing agents released [11,12], neural networks where neurons in brains of mild injury are capable of spontaneous healing by reinstating lost connections [13,14], cancer networks where cancer stem cells have the ability to self-renew (maintaining their undifferentiated state) and cause a relapse of the tumor in spite of conventional chemotherapies [15,16], and botnets where compromised hosts are able to autonomously become healthy after the scan of equipped antivirus softwares [17,18]. These indicate that the topology alone may not determine robustness [19], as the self-healing mechanisms help such complex systems maintain great stability routinely in the presence of continual small failures and shocks, for instance [20]. It is thus essential to incorporate the self-healing phenomenon and understand its consequences on network robustness.

Concerning robustness improvement against failures or attacks, a range of strategies have been reported, including edge rewiring or addition [21–24], edge swapping (while conserving the node degrees) [25,26], and even edge removal in the case of interdependent networks [27,28]. These strategies are applicable in technological (e.g., communication) networks, where backup channels and rerouting protocols are accessible. However, this is not the case with most infrastructure networks, since the creation of new physical links has geographic constraints, and incurs time and financial costs, if at all possible. The limitations are even inherent in biological and social systems, rendering these designed strategies virtually ineffective.

In this paper we study the case in which only previously existing links can be recovered due to self-healing of nodes. We work with a minimal model, as is often favored in physics, to investigate the impact of self-healing on robustness; i.e., we aim at being as generic as possible in the system description instead of proposing particular recovery algorithms [10]. We adopt the perspective of healing, yet we mention that our model might be motivated in other instances besides network healing as the system under consideration is static by nature. Albeit simple, the model we develop incorporates the network topology, failure or attack pattern, and the self-healing capability of nodes. It is found that the self-healing capability has a profound impact on the phase transition in the emergence of giant clusters, and the topology-dependent self-healing schemes display distinct behaviors in upholding integrity under random failures and intentional attacks.

II. RESULTS

To be concrete, we build our networks using the configuration model [29] that is a random graph with a specified degree distribution p_k, in the limit of large graph size. In the tradition of physics, this model is a natural choice for networks in the absence of any known geometry for the problem. It has become a standard arena for the exploration of network robustness [7,25,30,31], and this tradition is followed here. Our approach involves two quantities: (i) the probability q_k that a node is intact given that it has degree k, describing the error pattern; and (ii) the capability α_k of self-healing of a node given that it has degree k. We assume that any faulty node of degree k is recovered spontaneously together with random α_k proportion of incident edges connecting its intact neighbors [32]. Therefore, each node in the network is occupied (either *intact* or *recovered*): $\alpha_k \equiv 1$ means the strongest self-healing capability—an edge is occupied unless both end nodes are recovered ones, while $\alpha_k \equiv 0$ is the weakest—an edge is occupied only if both end nodes are intact. In the language of percolation [7], we are dealing with a bond

percolation, and interestingly, the case $\alpha_k \equiv 0$ is essentially equivalent to a site percolation except some isolated nodes.

A. Networks with constant self-healing capability

We start from a degree-independent scenario, i.e., $q_k = q$ and $\alpha_k = \alpha$ for all k. By construction, every node has degree k with probability p_k. Hence, the probability generating function of node degree is $G_0(x) = \sum_k p_k x^k$ [29]. If we follow a randomly chosen edge from a root node, the node reached, say, v_0, can be intact with probability q, or recovered with probability $1 - q$. In the first case, the selected edge is occupied with probability 1, while in the second case, it is occupied with mean probability αq [33]. Hence, the edge is occupied with probability $\rho := q + \alpha q (1 - q)$, and the distribution of the number of edges leading out of v_0 (namely, the excess degree distribution) is generated by [7]

$$F_1(x) = \frac{\sum_k k p_k \rho x^{k-1}}{\langle k \rangle} = \rho G_1(x), \qquad (1)$$

where $\langle k \rangle = \sum_k k p_k$ is the average degree, and $G_1(x) = G_0'(x)/\langle k \rangle$ is the generating function of excess node degree alone.

Let $H_1(x)$ be the generating function 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. Since the subclusters will not be connected in cycles for a sufficiently large random graph below percolation (namely, the graph has a pure branching structure), we may safely treat each subcluster independently of the others [29]. Thus, $H_1(x)$ satisfies the self-consistency condition

$$H_1(x) = [1 - F_1(1)] + x F_1[H_1(x)], \qquad (2)$$

where the first term corresponds to the probability that the selected edge is deleted (unoccupied), and the second term accounts for the size distribution of clusters attached to v_0. Analogously, the probability distribution of the size of cluster to which a randomly chosen node belongs is generated by $H_0(x)$, where

$$H_0(x) = 1 - \eta + \eta x G_0[H_1(x)], \qquad (3)$$

and $\eta := q + \alpha(1 - q)$ representing the probability that the node is either intact or recovered with α fraction of incident edges. An important quantity that can be deduced, for our present purpose, is $\langle s \rangle = H_0'(1)$, the mean size of cluster to which a random node belongs. Substituting (2) and (3), we find that

$$\langle s \rangle = \eta + \eta G_0'(1) H_1'(1) = \eta + \frac{\eta \rho G_0'(1)}{1 - \rho G_1'(1)}. \qquad (4)$$

The critical values (q_c, α_c) at which a giant (formally infinite) cluster first emerges, i.e., (4) diverges, are determined by

$$1 = [q_c + \alpha_c q_c (1 - q_c)] G_1'(1), \qquad (5)$$

where $G_1'(1)$ is the branching factor of the network. When $\alpha = 0$, the critical intactness probability $q_c = 1/G_1'(1)$, which coincides with [7, Eq. (12)] confirming the equivalence to the uniform site percolation as commented above. For a network with power-law degree distribution $p_k \sim k^{-\gamma}$, the ratio $\langle k^2 \rangle / \langle k \rangle = G_1'(1) + 1$ diverges when $1 \leqslant \gamma < 3$. By (5),
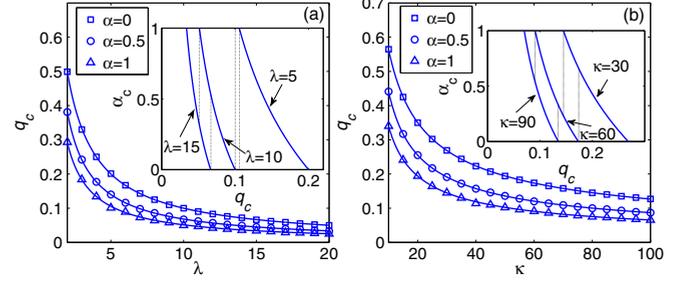

FIG. 1. (Color online) Main panels: percolation threshold q_c for networks of 10^6 nodes from numerical simulations with $\alpha = 0$ (squares), 0.5 (circles), and 1 (triangles), and exact solutions (solid lines) by (5): (a) for ER graphs with $\langle k \rangle = \lambda$, and (b) for scale-free networks with degree exponent $\gamma = 2.4$ and exponential cutoff κ. To obtain the data points q_c, we begin with $q = 0.99$ and mark each node of a given network as *recovered* with probability $1 - q$ independently, and delete all its incident edges (while we record its neighbor set). We then reconnect a random α fraction of *intact* neighbors for each *recovered* node [32]. After checking all nodes, we calculate the fraction (relative size) S of the giant cluster. We decrease q and repeat the process until $S < 10^{-3}$. The plots correspond to the average of 50 random graphs with 20 independent runs for each. Insets: α_c vs q_c by (5): (a) for ER graphs with $\lambda = 5, 10, 15$, and (b) for scale-free networks with $\gamma = 2.4$ and $\kappa = 30, 60, 90$.

$q_c \to 0$ for any α if $1 \leqslant \gamma < 3$. This means, as expected, that a scale-free network with any (uniform) self-healing capability is robust to random failure, reproducing the well-known result of Cohen *et al.* [8] in the case of $\alpha = 0$.

Equation (5) is confirmed by the numerical results shown in Fig. 1 for Erdős-Rényi (ER) random 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 degree distribution $p_k \sim k^{-\gamma} e^{-k/\kappa}$ ($k \geqslant 1$), which are ubiquitous in real-world complex systems [2]. As expected, an increase in the self-healing capability α systematically yields a decrease in the critical intactness probability q_c for all values of λ and κ. The "work" of α is better appreciated when turning to the insets of Fig. 1. For instance, an increase from $\alpha = 0$ to $\alpha \approx 0.5$ makes an ER graph with $\lambda = 10$ as robust as that with $\lambda = 15$ in terms of q_c; while an ER graph with $\lambda = 5$ can never (even having the strongest self-healing capability $\alpha = 1$) be as robust as that with $\lambda = 10$. Moreover, although the larger the λ (or κ), the smaller the gain of q_c (obtained by increasing α from 0 to 1), it does not mean that it would be always more difficult to change the robustness for denser ER graphs (or scale-free networks with larger cutoff). For example, a change of q_c from around 0.07 to around 0.05 demands a pronounced increase from $\alpha \approx 0.5$ to $\alpha = 1$ for an ER graph with $\lambda = 10$ but only needs an increase from 0 to around 0.3 for that with $\lambda = 15$ [see Fig. 1(a) inset].

On top of the percolation threshold, two important measures of network robustness are the fraction S of giant cluster above percolation and the robustness R [25], an integral of S over the entire depreciation process. Recall that Eq. (4) only applies below percolation where the largest cluster remains finite. However, we can still solve for S above the phase transition by evaluating $H_0(1)$ exclusively over finite clusters [29]. Using (2)

and (3), it follows that

$$S = 1 - H_0(1) = \eta[1 - G_0(u)], \tag{6}$$

where $u = H_1(1)$ is the smallest non-negative solution of $1 - u = \rho[1 - G_1(u)]$. Accordingly, the mean size of the clusters, excluding the giant cluster to which a randomly chosen node belongs, can be expressed by

$$\langle s \rangle = \frac{H_0'(1)}{H_0(1)} = \frac{\eta}{1-S}\left[G_0(u) + \frac{\rho G_0'(u) G_1(u)}{1 - \rho G_1'(u)}\right], \tag{7}$$

which reduces to (4) in the absence of giant cluster, namely, $S = 0$ and $u = 1$. The robustness R, attracting increased attention [25–27,31], on the other hand, is defined as

$$R = \frac{1}{N}\sum_{qN=1}^{N} S(q) \sim \int_0^1 S(q)\,dq, \tag{8}$$

where N is the number of nodes in the network and $S(q)$ is the fraction of nodes in the largest connected cluster after recovering qN nodes [34] [in particular, $S(q)$ is given by (6) under random failures]. Figure 2 shows the variations of S and R under random failures as well as targeted attacks, which we will explain later.
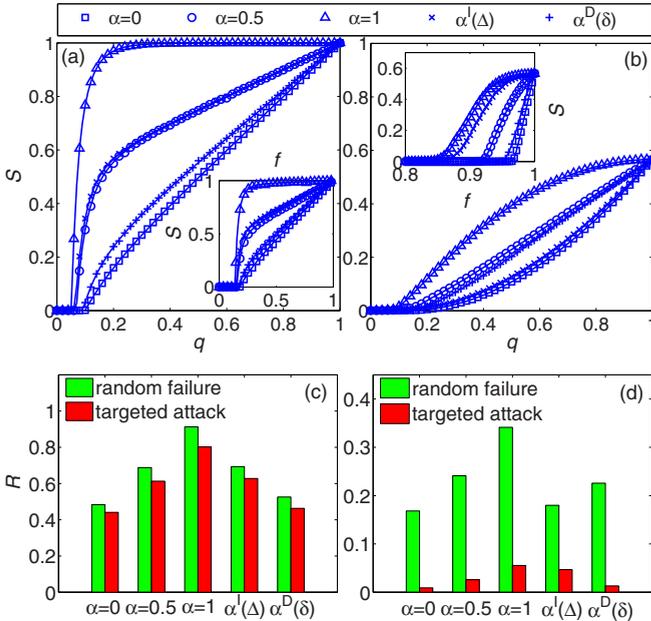

FIG. 2. (Color online) First row [(a) and (b)] main panels: fractions of giant clusters S as functions of q for $\alpha = 0$ (squares), 0.5 (circles), 1 (triangles), and $\alpha^I(\Delta)$ (crosses), and $\alpha^D(\delta)$ (pluses). Panel (a) is for ER graphs with $\lambda = 10$; (b) is for scale-free networks with $\gamma = 2.4$ and $\kappa = 60$. The insets show, respectively, S vs f, the fraction of the least connected nodes that are kept intact. Data points correspond to the simulation results averaged over 50 random graphs with 20 independent runs for each, and solid lines are the exact solutions using (6), (9), (10), and (11). Second row [(c) and (d)]: robustness R of networks with different self-healing schemes under random failures and targeted attacks: (c) corresponds to (a), and (d) corresponds to (b).

B. Networks with degree-dependent self-healing capability

To further explore the robustness variation in response to different failure patterns as well as self-healing capabilities, we consider the general degree-dependent scenario hereafter. Now if we follow a randomly chosen edge from a root node with degree k' to a node, say, v_0, with degree k, the probability that the selected edge is occupied turns out to be $\rho_{k,k'} := q_k + \alpha_k q_{k'}(1 - q_k)$, and the excess degree distribution is generated by

$$F_1(x|k') = \frac{\sum_k k p_k \rho_{k,k'} x^{k-1}}{\langle k \rangle}. \tag{9}$$

in analogy to (1). Likewise, the counterparts of (2) and (3) become, respectively,

$$H_1(x|k') = 1 - F_1(1|k') + \frac{x\sum_k k p_k \rho_{k,k'} H_1(x|k)^{k-1}}{\langle k \rangle} \tag{10}$$

and

$$H_0(x) = 1 - \sum_k p_k \eta_k + \sum_k p_k \eta_k H_1(x|k)^k, \tag{11}$$

where $\eta_k = q_k + \alpha_k(1 - q_k)$.

We now apply these results to the study of network robustness in various nonuniform cases. We consider two types of topology-dependent self-healing capabilities signified by $\alpha^I(k_c) := \alpha_k = k/\max\{k, k_c\}$ and $\alpha^D(k_c) := \alpha_k = \min\{k, k_c\}/k$, where k_c is an integer ranging from the minimum degree δ to the maximum degree Δ of the network. We assume $\delta \geqslant 1$ without loss of generality. The first type $\alpha^I(k_c)$ indicates a recovery scheme where hubs possess the strongest self-healing capability, while the second type $\alpha^D(k_c)$ implies that the least connected nodes have the strongest self-healing capability. These schemes allow one to interpolate smoothly between uniform and nonuniform self-healing capabilities (see Appendix A).

Figure 2 reports the fraction of giant cluster S and robustness index R for the same networks used in Fig. 1. The main panels in Figs. 2(a) and 2(b) display the behaviors under random failures, where a fraction $1 - q$ of random nodes are selected as *recovered*, and their incident edges are reconnected according to the respective self-healing schemes. The insets in Figs. 2(a) and 2(b) display the behaviors under intentional attacks targeted at hubs (or systemic failures inclined toward hubs). Here, the targeted attack is equivalent to setting $q_k = \theta(k - k_a)$, where θ is the Heaviside step function and k_a is a cutoff ranging from 0 to the maximum degree of the network [7]. We define $f = f(k_a)$, the fraction of the least connected nodes that are kept intact, by the number of intact nodes with degree smaller than k_a divided by 10^6, the total number of nodes. By doing so, f plays an analogous role as q in the random failure case, facilitating our comparison.

The results gathered in Fig. 2 allow us to draw several interesting comments. First, the simulated results agree well with theoretical predictions. The phase transition point at $S \sim 0$, as expected, coincides with the critical probability q_c in Fig. 1 for $\alpha = 0$, 0.5, and 1. Second, there is a pronounced difference on the convexity of S curves for $\alpha = 0$, 0.5, and 1, in both ER [Fig. 2(a)] and scale-free networks [Fig. 2(b)]. The increase of self-healing capability in terms of α yields

a noticeable increase in the fraction of giant clusters. For example, consider $q = 0.2$ in Fig. 2(a), namely, 20% nodes in the network are intact. The giant cluster consists of only 15% nodes for $\alpha = 0$ but consists of almost all nodes for $\alpha = 1$, dramatically enhancing the network robustness. Third, for ER graphs, the topology-dependent self-healing scheme $\alpha^I(\Delta)$ produces results very close to the uniform case $\alpha = 0.5$ in both random failures and targeted attacks [Figs. 2(a) and 2(c)]. Additionally, the self-healing scheme $\alpha^D(\delta)$ is similar to the case $\alpha = 0$ in both random failures and targeted attacks [Figs. 2(a) and 2(c)].

These phenomena can be explained as follows. In the random failure scenario, we have $\alpha^I(\Delta) = k/\Delta \sim \langle k \rangle / \Delta \sim 0.5$ and $\alpha^D(\delta) = \delta/k \sim \delta/\langle k \rangle \sim 0.1$ due to the bell-shaped degree distribution of ER graphs. The similarity of the results between random failures [e.g., Fig. 2(c) green bars] and targeted attacks [e.g., Fig. 2(c) red bars] stems from the homogeneity of the network topology. In other words, the robustness of ER networks is not sensitive to the individual variation of self-healing capability—only the overall average change matters.

However, it is a quite different story when it comes to scale-free networks. In the random failure scenario [Fig. 2(b) main panel], the fraction of giant cluster S for $\alpha^D(\delta)$ is slightly smaller than that for $\alpha = 0.5$; while S for $\alpha^I(\Delta)$ is slightly larger than that for $\alpha = 0$, confirmed by R [Fig. 2(d) green bars]. This is due to the fact that most nodes in a scale-free network have small degrees and only a small number of nodes (hubs) have large degrees. Therefore, a random recovered node probably has a small degree, whose self-healing capability is higher under the $\alpha^D(\delta)$ scheme, rendering a more robust network, than under the $\alpha^I(\Delta)$ scheme. Namely, the self-healing capability of small-degree nodes largely determines robustness in the random failure scenario, while increasing the self-healing capability for hubs has a quite limited contribution. In sharp contrast, under targeted attacks, the self-healing scheme $\alpha^I(\Delta)$ turns out to improve robustness much more effectively than the $\alpha^D(\delta)$ scheme. For example, the red bars in Fig. 2(d) show that $R(\alpha = 1) \sim R[\alpha^I(\Delta)] \sim 0.05 \gg R[\alpha^D(\delta)] \sim 0.015$. This is again due to the heterogeneity of scale-free networks—the self-healing capability becomes more critical for hubs than for small-degree nodes in this case.

When comparing the random failure and targeted attack scenarios, we note that a scale-free network with maximum self-healing capability (i.e., $\alpha = 1$) under targeted attacks appears even more fragile, in terms of S as well as R, than that without self-healing capability (i.e., $\alpha = 0$) under random failures. This is unforseen yet reasonable because the hubs can be strongly connected with each other, which is known as the
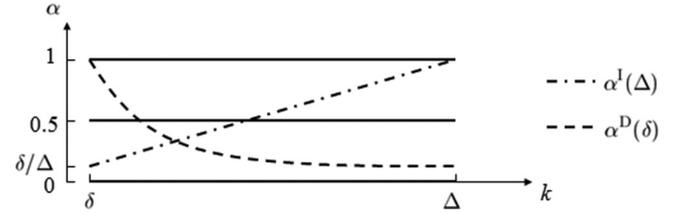

FIG. 3. Illustration of several different self-healing capability distributions. For $\alpha^I(k_c)$, the capability increases with respect to node degree, while for $\alpha^D(k_c)$, the capability decreases with respect to node degree. Moreover, $\alpha^I(k_c)$ with $k_c = \delta$ is equivalent to $\alpha^D(k_c)$ with $k_c = \Delta$—they are both equivalent to the uniform self-healing scheme $\alpha_k \equiv \alpha = 1$.

rich-club phenomenon [35,36]—removing the edges between them may cause rapid fragmentation of the entire network.

It is worth adding that the scale-free networks in our examples seem often to have higher q_c (cf. Fig. 1) and lower S (cf. Fig. 2), and are less robust than the ER graphs. This is because the mean degree of the scale-free networks is lower. For instance, the mean degree of the scale-free network in Fig. 2(b) with $\gamma = 2.4$ and $\kappa = 60$ is below 3, while that of the ER graph in Fig. 2(a) is 10.

Finally, we apply our theory to varied real-world networks, and find that the impact of self-healing capability on network robustness can be qualitatively predicted (see Appendix B).

III. DISCUSSION

Self-healing phenomenon plays an important role in many complex systems. Yet, little was known about how it will affect robustness in complex networks. We have here developed analytical tools to deal with this problem using degree distribution as the only input. Our key finding, that the self-healing capability has a profound impact on both percolation transitions and (integrated) fraction of giant clusters for homogeneous and heterogeneous topologies, suggests a simple local mechanism to better understand network robustness which goes beyond merely network topology. A number of variants of the problem are of interest. For instance, in some cases the attacks are not launched simultaneously but in a sequential manner. There could also be self-healing time delays in response to failures. Moreover, the role of self-healing functions in networks with degree-degree correlation is certainly worth investigation. We hope the results presented here could stimulate further research efforts on these related issues which have practical implications for designing robust systems in the real world.

TABLE I. List of five empirical networks analyzed in this paper. N: number of nodes; M: number of edges.

	N	M	Description
USPowerGrid [5]	4941	6594	Power grid of the western United States
ca-CondMat [37]	23133	186936	Collaboration network of arXiv Condensed Matter
Yeast [38]	2361	7182	Protein-protein interactions in the yeast *S. cerevisiae*
C. elegans [5,39]	297	2148	Neural network of the worm *C. elegans*
Facebook [40]	4039	88234	Facebook user-user friendships

TABLE II. Robustness index R of five empirical networks with various self-healing schemes in the case of random failures as well as targeted attacks.

	Random failure					Targeted attack				
	$\alpha = 0$	$\alpha = 0.5$	$\alpha = 1$	$\alpha^I(\Delta)$	$\alpha^D(\delta)$	$\alpha = 0$	$\alpha = 0.5$	$\alpha = 1$	$\alpha^I(\Delta)$	$\alpha^D(\delta)$
USPowerGrid	0.227	0.312	0.420	0.249	0.293	0.063	0.087	0.104	0.096	0.071
ca-CondMat	0.405	0.491	0.570	0.429	0.488	0.083	0.109	0.131	0.124	0.095
Yeast	0.391	0.472	0.556	0.408	0.463	0.109	0.122	0.136	0.129	0.118
C. elegans	0.477	0.580	0.701	0.492	0.523	0.331	0.386	0.430	0.425	0.347
Facebook	0.452	0.536	0.670	0.478	0.510	0.113	0.138	0.162	0.151	0.124

APPENDIX A: ILLUSTRATION OF SELF-HEALING CAPABILITIES

In Fig. 3 several different self-healing capability distributions are presented.

APPENDIX B: IMPACT OF SELF-HEALING CAPABILITY ON REAL NETWORKS

We studied the impact of self-healing capacity on network robustness for diverse empirical networks (see Table I for a brief description): namely, USPowerGrid [5], the vertices being generators, transformers, and substations and the edges being high-voltage transmission lines; ca-CondMat [37], the edges in this network indicating that the two scientists co-authored at least one paper; Yeast [38], the vertices being proteins and the edges representing biological interactions; C. elegans [5,39], the vertices being neurons and the edges being neural connections; Facebook [40], the edges in this network indicating that the two users are friends on Facebook. All these five networks except USPowerGrid are demonstrated to have power-law degree distributions. USPowerGrid does not have a power-law regime but has an exponential decaying tail.

The robustness indices R of these networks under random failures and targeted attacks are summarized in Table II. The results are broadly consistent with our theory and synthetic models. For example, an increase in self-healing capability α systematically yields an increase in R. It is interesting to see that our found signature of scale-free networks—$R[\alpha^D(\delta)] > R[\alpha^I(\Delta)]$ under random failures, while $R[\alpha^I(\Delta)] > R[\alpha^D(\delta)]$ under targeted attacks—is obeyed by all five systems. We contend that this phenomenon for USPowerGrid may find its origins in the heterogeneity of the degrees. Although USPowerGrid has a narrower degree distribution than a scale-free network, the exponential decaying is much slower than a Poisson degree distribution of an ER random graph.

[1] M. E. J. Newman, SIAM Rev. **45**, 167 (2003).

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

[3] A.-L. Barabási and R. Albert, Science **286**, 509 (1999).

[4] P. Erdős and A. Rényi, Publ. Math. Inst. Hung. Acad. Sci. **5**, 17 (1960).

[5] D. J. Watts and S. H. Strogatz, Nature (London) **393**, 440 (1998).

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

[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] A. Majdandzic, B. Podobnik, S. V. Buldyrev, D. Y. Kenett, S. Havlin, and H. E. Stanley, Nat. Phys. **10**, 34 (2014).

[11] S. R. White, N. R. Sottos, P. H. Geubelle, J. S. Moore, M. R. Kessler, S. R. Sriram, E. N. Brown, and S. Viswanathan, Nature (London) **409**, 794 (2001).

[12] K. S. Toohey, N. R. Sottos, J. A. Lewis, J. S. Moore, and S. R. White, Nat. Mater. **6**, 581 (2007).

[13] M. Desmurget, F. Bonnetblanc, and H. Duffau, Brain **130**, 898 (2007).

[14] R. J. Nudo, Front. Hum. Neurosci. **7**, 887 (2013).

[15] C. E. Meacham and S. J. Morrison, Nature (London) **501**, 328 (2013).

[16] A. Kreso and J. E. Dick, Cell Stem Cell **14**, 275 (2014).

[17] Y. Shang, Appl. Math. Inf. Sci. **6**, 29 (2012).

[18] P. Barford and V. Yegneswaran, in *Malware Detection: Advances in Information Security* (Springer-Verlag, New York, 2007), pp. 171–191.

[19] It is also well documented that, in infrastructure networks handling physical flows, capacity or load plays a role in robustness [41,42].

[20] C. W. Cotman and M. Nieto-Sampedro, Annu. Rev. Psychol. **33**, 371 (1982).

[21] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, Physica A **357**, 593 (2005).

[22] W. Quattrociocchi, G. Caldarelli, and A. Scala, PLoS ONE **9**, e87986 (2014).

[23] Y. Shang, Int. J. Nonlinear Sci. Numer. Simul. **14**, 355 (2013).

[24] X. B. Cao, C. Hong, W. B. Du, and J. Zhang, Chaos Solitons Fractals **57**, 35 (2013).

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

[26] A. Zeng and W. Liu, Phys. Rev. E **85**, 066130 (2012).

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

[28] R. Parshani, S. V. Buldyrev, and S. Havlin, Phy. Rev. Lett. **105**, 048701 (2010).

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

[30] A. A. Moreira, J. S. Andrade Jr, H. J. Herrmann, and J. O. Indekeu, Phys. Rev. Lett. **102**, 018701 (2009).

[31] Y. Shang, Phys. Rev. E **90**, 032820 (2014).

[32] The model is independent of the order of node recovery.

[33] A mean-field approximation gives $\mathbb{P}$(root connected to v_0) = $\alpha \cdot \mathbb{P}$(root intact) + $0 \cdot \mathbb{P}$(root recovered) = αq.

[34] The original definition [25] of R is slightly modified here by considering *recovered* nodes instead of *removed* nodes.

[35] F. Colizza, A. Flammini, M. A. Serrano, and A. Vespignani, Nat. Phys. **2**, 110 (2006).

[36] This might seem at odds with the fact that scale-free networks tend to exhibit disassortativity. However, they do not conflict with each other: Although the chance of finding a chain of peripheral, low-degree nodes is low, the hubs can be interconnected with each other [43].

[37] J. Leskovec, J. Kleinberg, and C. Faloutsos, ACM Trans. Knowl. Discov. Data **1**, 2 (2007).

[38] H. Jeong, S. Manson, A.-L. Barabási, and Z. Oltvai, Nature (London) **411**, 41 (2001).

[39] J. White, E. Southgate, J. Thomson, and S. Brenner, Philos. Trans. R. Soc. London B **314**, 1 (1986).

[40] J. McAuley and J. Leskovec, in *Advances in Neural Information Processing Systems* (NIPS, Lake Tahoe, 2012), pp. 548–556.

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

[42] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, and D. Helbing, Phys. Rev. Lett. **100**, 218701 (2008).

[43] S. Zhou and R. J. Mondragón, New J. Phys. **9**, 173 (2007).