Scaling of percolation transitions on Erdös-Rényi networks under centrality-based attacks

Nahuel Almeira [1,2,*] Orlando Vito Billoni [1,2,†] and Juan Ignacio Perotti [2]
[1]*Facultad de Matemática, Astronomía, Física y Computación, Universidad Nacional de Córdoba*
Ciudad Universitaria, 5000 Córdoba, Argentina
[2]*Instituto de Física Enrique Gaviola (IFEG-CONICET) Ciudad Universitaria, 5000 Córdoba, Argentina*

The study of network robustness focuses on the way the overall functionality of a network is affected as some of its constituent parts fail. Failures can occur at random or be part of an intentional attack and, in general, networks behave differently against different removal strategies. Although much effort has been put on this topic, there is no unified framework to study the problem. While random failures have been mostly studied under percolation theory, targeted attacks have been recently restated in terms of network dismantling. In this work, we link these two approaches by performing a finite-size scaling analysis to four dismantling strategies over Erdös-Rényi networks: initial and recalculated high degree removal and initial and recalculated high betweenness removal. We find that the critical exponents associated with the initial attacks are consistent with the ones corresponding to random percolation. For recalculated high degree, the exponents seem to deviate from mean field, but the evidence is not conclusive. Finally, recalculated betweenness produces a very abrupt transition with a hump in the cluster size distribution near the critical point, resembling some explosive percolation processes.

I. INTRODUCTION

The study of percolation in complex networks is a current research topic that has both theoretical inquires [1,2] and practical applications. Percolation transitions are observed in many biological, social, and technological complex networks [3,4] and are connected to the problem of resilience to damage [5–8] and therefore to the functionality of the systems associated with the networks. Also, theoretical tools devised for the analysis of percolation have been used in the study of disease spreading [9], city traffic dynamics [4], and the structural characterization of networks [10], among others. In particular, mathematical models for percolation processes on interdependent graphs were developed [11] to capture salient features of random failures of systems such as power grids.

Failures are usually modeled as random deletions of nodes or links, while in attacks influential nodes or links are removed according to a rank of specific characteristics, trying to produce the largest damage to the network. The effectiveness of the attack strategy depends on the topological features of the network as well as on the type of attack. For this reason, several network architectures were studied under different strategies to evaluate both the robustness of networks and the effectiveness of attacks [12–14]. In the pioneering work of Holme, *et al.* [12], the effect of different centrality edge- and node-based attacks was studied in several synthetic and real-world networks. Later, Iyer *et al.* [13] extended these results by studying new centrality measures and network models for the case of node-based attacks. In a recent study performed by Wandelt *et al.* [14], an extensive benchmark of synthetic and real-world networks was analyzed using different dismantling strategies providing the most extensive comparative analysis on network robustness up to now.

It is widely known that scale-free networks are fragile against centrality targeted attacks [12,15–17] but robust against random failures [17]. On the other hand, networks with homogeneous degree distribution, such as Erdős-Rényi (ER) networks, are expected to be robust under targeted attacks. In particular, they have been proved to be robust against degree-based attacks [18]. However, some networks are fragile to targeted attacks despite having homogeneous degree distributions. One such example is the US power grid, which exhibits a significant connectivity loss when nodes with high load are deleted [19]. Another example is the Watts-Strogatz model of small-world homogeneous networks, which have been proved to be particularly fragile in a cascading failure scenario. Xia *et al.* [20] attributed the fragility of these networks to their heterogeneous betweenness distribution. Attacks based on betweenness are among the most efficient ways to dismantling a network [7,12–14] and are particularly effective in networks having a heterogeneous betweenness distribution. However, in Erdős-Rényi networks, where both degree and betweenness distributions are homogeneous [20,21], a betweenness-based attack is not expected to outperform other targeted attacks. As we will show in this article, this is not the case. In particular, the recalculated version of the betweenness-based attack on nodes is particularly effective to destroy ER networks, with a performance comparable to the most efficient methods to dismantle networks [22,23].

In this work, we study percolation processes on ER networks under different attack strategies using finite-size scaling analysis to assess the nature of the transition towards the fragmented phase. Our results show that the choice of the attack strategy can change the properties of the transition.

In particular, the transition produced by the recalculated betweenness-based attack is sharper than for the rest of the attacks, deviating significantly from the random percolation universality class. Given the steep variation of the order parameter near the transition, we consider the process as a case of "explosive percolation" [24–26]. The results of the finite-size scaling analysis are consistent with a continuous phase transition, but we cannot determine that this result holds in the infinite-size limit.

A. Attack strategies

In centrality-based attacks, nodes are sorted in decreasing order according to a centrality measure. Then, they are sequentially removed according to that list (ties, if any, are usually broken randomly). There is an extensive list of centrality measures that have been tested in multiple networks (see, for example, Ref. [13]). Some of the most popular are degree, betweenness [27], closeness, eigenvector, and collective influence [23]. In general, when a node is removed, the centrality values of the remaining nodes change. Thus the attack can be improved by recomputing the list after each removal step. If the centrality measure uses only local information, like degree or collective influence, only a fraction of nodes will eventually change, so the original ordering of the nodes may remain the same after several steps. On the other hand, measures like betweenness or eigenvector centrality use global information, so even the deletion of a single node can potentially change the ordering in a significant way. Given that the *recalculated* version of an attack uses more updated information of the network, it is in general more efficient than its *initial* counterpart [13].

In this work, we will focus on both the initial and recalculated versions of the attacks based on two centrality measures: degree and betweenness. The degree of a node, defined as the number of neighbors the node has, is the most intuitive centrality measure and one of the most studied in the literature. It is easily interpreted in terms of network connectivity and it has the advantage of being a local measure, which makes it suitable for analytical treatment. On the other hand, betweenness centrality is a global measure and is defined in the following way. Let $\sigma(s, t)$ be the number of shortest paths connecting nodes s and t and let $\sigma_i(s, t)$ be the number of such paths going through node i. Then, the betweenness centrality of node i is

$$b_i = \sum_{s \neq t} \frac{\sigma_i(s, t)}{\sigma(s, t)}, \tag{1}$$

where we adopt the convention that $\sigma_i(s, t)/\sigma(s, t) = 0$ if both $\sigma_i(s, t)$ and $\sigma(s, t)$ are zero.

Betweenness can be thought of as the amount of load a node must support when there is some kind of flux on the network. Nodes with higher betweenness articulate different groups of nodes and their importance is more related to the communicability of the network. In particular, it is easy to check that nodes with degree lower than two have betweenness equal to zero. Being a global measure, it is hard to compute this centrality. The most efficient algorithm so far known was proposed by Brandes *et al.* in [28] and runs in $O(NM)$, where N and M are the number of nodes and links

in the network, respectively. The main reason for considering this measure is that it has been reported as the most efficient attack strategy for many networks, including both synthetic and real-world networks [13,14].

B. Percolation

Site percolation in complex networks can be stated by considering that each node of the network can be either *occupied*, with probability p, or *unoccupied*, with probability $1 - p$. Only occupied nodes can be connected; thus links connecting at least one unoccupied node are also considered unoccupied. If $p = 0$, the network is empty and, if $p = 1$, the original network is recovered. When the occupation probability is small, occupied nodes belong to different small-sized components, but above a critical value $p = p_c$, one of the components acquires an extensive size. At this point, it is said that the system percolates. The extensive component is known as the *giant connected component* (GCC) and the critical point is referred to as the *percolation threshold*.

Let N be the size of the network and N_1 the size of the GCC. In the thermodynamic limit $N \to \infty$, percolation theory states that the relative size $S_1 = N_1/N$ follows the critical behavior

$$S_1 = \begin{cases} 0, & p < p_c, \\ a(p - p_c)^\beta, & p \geqslant p_c, \end{cases} \tag{2}$$

where a is a proportionality constant and $\beta > 0$ is the critical exponent associated with S_1. The transition between the percolated and nonpercolated state has been widely studied in statistical physics, and it has been shown to exhibit a continuous transition in many different network models. In this framework, S_1 is considered the order parameter of the transition.

As it occurs in continuous transitions, other measures also manifest a critical behavior near the percolation threshold. One such measure is the average cluster size, which plays the role of susceptibility and is computed as

$$\langle s \rangle = \frac{\sum_s' s^2 n_s(p)}{\sum_s' s n_s(p)}, \tag{3}$$

where $n_s(p)$ is the number of clusters of size s per node and the primed sum excludes the GCC. At the critical point, $\langle s \rangle$ diverges in the thermodynamic limit as $\langle s \rangle \sim |p - p_c|^{-\gamma}$, with $\gamma > 0$. Also, $n_s(p)$ has its own critical behavior and close to p_c it becomes very heterogeneous, being well described by the expression

$$n_s(p) \sim s^{-\tau} e^{-s/s^*}. \tag{4}$$

Here s^* represents the characteristic cluster size, which scales as $s^* \sim |p - p_c|^{-1/\sigma}$. Then, at $p = p_c$ the number of clusters of size s follows a power law $n_s(p) \sim s^{-\tau}$. Finally, the correlation length ξ, defined as the geometrical length of a typical cluster, scales as $\xi \sim |p - p_c|^{-\nu}$, where $\nu > 0$ [29].

The theory of critical phenomena states that continuous transitions can be fully characterized by its critical exponents. If the same exponents are shared between two systems, they belong to the same universality class. In percolation only two exponents are independent, and the others can be derived

using different scaling relations. For example, the exponent associated with the cluster size distribution can be obtained as [29]

$$\tau = 2 + \frac{\beta}{\gamma + \beta}. \tag{5}$$

As β and γ are both positive, Eq. (5) shows that $\tau \geqslant 2$. Another useful relation is given by [30,31]

$$2\frac{\beta}{\bar{\nu}} + \frac{\gamma}{\bar{\nu}} = 1, \tag{6}$$

where $\bar{\nu} = d\,\nu$ and d is the effective dimension of the network.

Standard site percolation on Erdős-Rényi graphs reports the mean-field exponents, with $\beta = \gamma = 1$, $\bar{\nu} = 3$, $\sigma = 1/2$, and $\tau = 5/2$ [32,33]. Also, in uncorrelated networks, the percolation threshold is given by [34]

$$p_c = \frac{1}{\kappa - 1}, \tag{7}$$

where $\kappa = \langle k^2 \rangle / \langle k \rangle$ is the heterogeneity parameter of the degree distribution.

From a theoretical point of view, standard percolation and node removal are different processes [17]. Percolation is an equilibrium reversible process, well described by the equilibrium statistical physics. On the other hand, node removal under specific attacks are irreversible processes such as the evolving rules that turn out in explosive percolation transitions [25]. Being aware of this, we relate the percolation probability p with a node removal procedure in which a fraction $f = 1 - p$ of nodes was removed. Using this relation we can apply the tools provided by percolation theory to the attack strategies previously described.

II. RESULTS

A. Percolation transition

Figure 1 shows the evolution of the size of the giant component as a function of the fraction of removed nodes f on an ER network with mean degree $\langle k \rangle = 5$. Each curve, which is an average taken over 10^3 independent networks, corresponds to a different attack, namely recalculated betweenness (RB), recalculated degree (RD), initial betweenness (IB), initial degree (ID), and random removal (Rnd). When a small network is considered [Fig. 1(a)], it can be seen that ID performs slightly better than IB, in the sense that, for each fraction of nodes removed the network is consistently more fragmented when nodes with high degree are removed. As it has been previously reported by Iyer *et al.* in [13], the situation reverts when the list of nodes is recalculated after each node removal, with RB outperforming RD. When a bigger network with the same characteristics is attacked [Fig. 1(b)], all the transitions become sharper. Except perhaps for RB, all the curves seem to be consistent with a continuous percolation transition. The curve for recalculated betweenness, on the other side, exhibits a very abrupt collapse at $f \approx 0.3$, with a very steep slope. Interestingly, for lower values of f this attack performs poorly (see inset), barely outperforming random removal. In fact, at the beginning both attacks (RB and Rnd) do not produce a network fragmentation as can be seen when compared to the
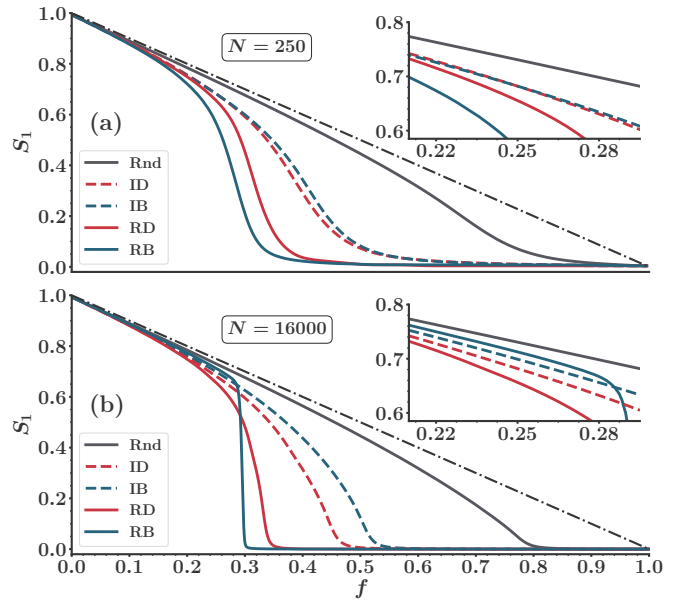

FIG. 1. Relative size of the giant component as a function of the fraction of removed nodes, averaged over 10^3 realizations, for two ER networks with $\langle k \rangle = 5$ and size N. As a reference, the dot-dashed line corresponds to node removal of a fully connected graph. The inset zooms the behavior right before the collapse produced by RB. (a) $N = 250$; (b) $N = 16000$.

attack of a fully connected graph in which the network is reduced one node at a time.

B. Finite-size scaling analysis

Finite-size scaling analysis is one of the most important tools in the study of continuous phase transitions and in particular to obtain the associated critical exponents [31,35,36]. According to this theory, the divergence of the correlation length at the critical point implies that every variable of the system becomes scale-independent at this point. For a finite-size system of size N, this produces a scaling of the form

$$X \sim N^{-\omega/\bar{\nu}} F[(f - f_c)N^{1/\bar{\nu}}], \tag{8}$$

where ω is an exponent related to the variable X. For $f = f_c$, the variable behaves as $X \sim N^{-\omega/\bar{\nu}}$. This relation holds asymptotically, i.e., in the limit $N \to \infty$ and $f \to f_c$, and it can be used to obtain the ratio $\omega/\bar{\nu}$ by computing $X(f_c, N)$ for different system sizes. In addition, the plot of $N^{\omega/\bar{\nu}} X$ as a function of $(f_c - f)N^{1/\bar{\nu}}$ yields to the universal function F, which does not depend on N, so curves corresponding to different sizes collapse.

In this work, we make use of two scaling relations. The first one is the scaling of the cluster relative sizes, which can be stated as [36]

$$S_i(f, N) \sim N^{-\beta/\bar{\nu}} \bar{S}_i[(f - f_c)N^{1/\bar{\nu}}]. \tag{9}$$

Here, the subscript $i = 1, 2, \ldots$ indicates the rank of each component, sorted by size in decreasing order. In particular, we will be interested in the order parameter S_1 and in the size of the second cluster $S_2 N$. The second scaling relation
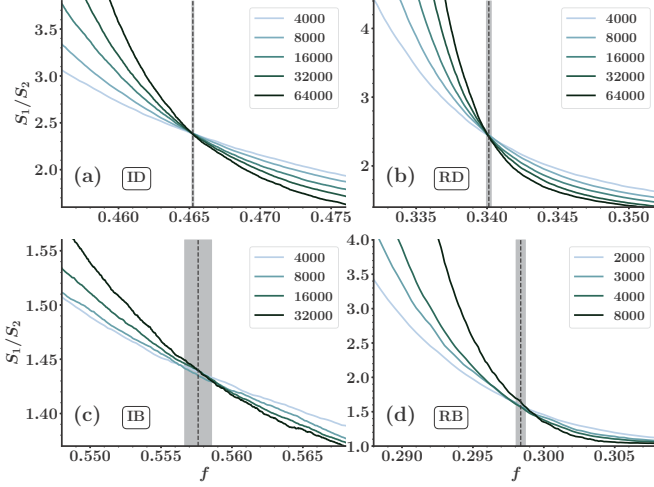
FIG. 2. Determination of the critical point f_c through the crossing-point method for the four attack strategies considered. Each curve represents an average over N_s independent realizations. The vertical line corresponds to the mean of the intersections and the shadowed region to the standard deviation. The values obtained are shown in Table I. (a) ID, $N_s = 2 \times 10^4$; (b) RD, $N_s = 2 \times 10^4$; (c) IB, $N_s = 2 \times 10^4$; (d) RB, $N_s = 5 \times 10^3$.

involves the average cluster size and can be stated as

$$\langle s \rangle (f, N) \sim N^{\gamma/\bar{\nu}} \tilde{S}[(f - f_c) N^{1/\bar{\nu}}]. \tag{10}$$

The percolation threshold f_c can be determined in several ways (for some of them, see [37]). The alternative we used in our work, which we call the crossing-point method, is the following. We first define $S_{ic}(N) \equiv S_i(f_c, N)$. According to Eq. (9), we have

$$S_{ic}(N) \sim N^{-\beta/\bar{\nu}} \tilde{S}_i(0). \tag{11}$$

Now we take the relative size of the first two components for a given size N and compute the quotient between them. The resulting expression becomes $S_{1c}(N)/S_{2c}(N) \sim \tilde{S}_1(0)/\tilde{S}_2(0)$, which is independent of N. This result implies that, at the critical point $f = f_c$, the curves of $S_1(f, N)/S_2(f, N)$ for different sizes should take the same value. The crossing-point method consists of numerically estimating the intersection of these curves. Using averages over 2×10^4 independent networks for the attacks ID, RD, and IB and over 5×10^3 independent networks for RB, we computed the quotients $S_1(f, N)/S_2(f, N)$ for different sizes and then calculated the values of the intersections for each pair of sizes. The value of f_c that we report is the mean of these intersections, with the standard deviation as the associated uncertainty. The method, applied to the four attack strategies previously described, is shown in Fig. 2. As it can be seen in the figure, the performance of the method depends on the nature of the attack. For the two degree-based attacks, the intersections occur with a very low variance, so the percolation threshold can be estimated with a very high precision as $f_c^{(\text{ID})} = 0.4652(7)$ and $f_c^{(\text{RD})} = 0.3401(2)$. The initial betweenness-based attack, on the other hand, has a lower precision, and the value obtained was $f_c^{(\text{IB})} = 0.558(1)$. The method also performs very well for the recalculated betweenness-based attack, even when the sizes and number of simulations that were used are lower,
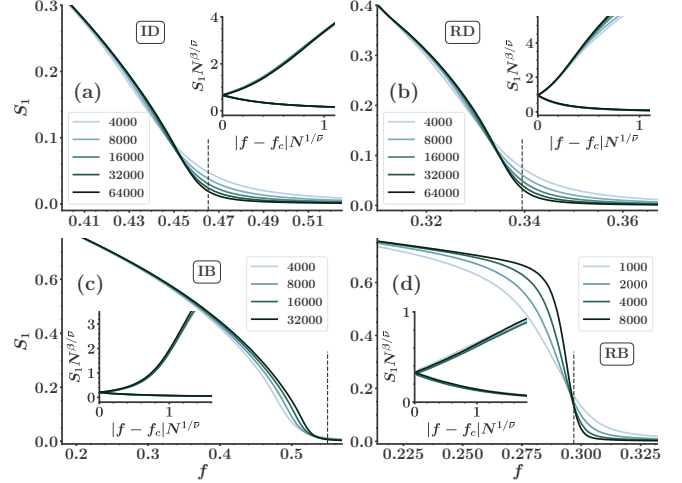

FIG. 3. Order parameter S_1 as a function of the fraction of nodes removed f in the neighborhood of the critical point. Each panel corresponds to one of the four attack strategies studied. Data is averaged over N_s independent realizations. The dashed vertical lines correspond to the value of the percolation threshold computed using the crossing method (see main text). The insets show the collapse of the curves using the scaling ansatz given by Eq. (9). The values for the percolation thresholds and critical exponents used to perform the scaling are the ones summarized in Table I. (a) ID, $N_s = 2 \times 10^4$; (b) RD, $N_s = 2 \times 10^4$; (c) IB, $N_s = 2 \times 10^4$; (d) RB, $N_s = 5 \times 10^3$.

due to its high computational complexity, giving an estimated percolation threshold of $f_c^{(\text{RB})} = 0.2984(2)$. From a dismantling point of view, the recalculated versions of the attacks are more effective than their initial counterparts, since they have lower percolation thresholds. In particular, the initial version of the betweenness-based attack is a rather poor dismantling strategy, being closer to random node removal than the rest of the attacks. On the other hand, the recalculated version of this attack is the most efficient one, performing better or comparable with other state-of-the-art dismantling strategies [22,23].

Once the percolation threshold has been estimated, we proceed to study the order parameter, susceptibility, and second cluster size in the vicinity of the transition. The four panels of Fig. 3 show the order parameter S_1 as a function of the fraction of nodes removed. Each panel corresponds to a different attack and each curve in the main panels corresponds to a different system size. It can be seen that the transitions

TABLE I. Numerical estimation of the percolation thresholds and critical exponents for the different attacks in ER networks with $\langle k \rangle = 5$ using finite-size scaling. The values of τ between brackets were computed using Eq. (5).

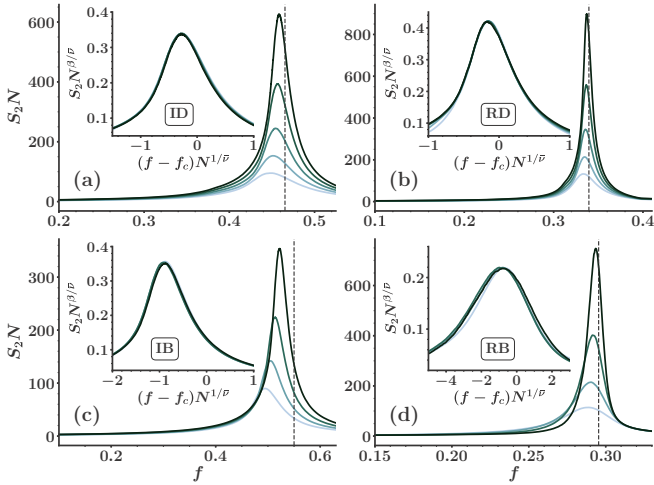|	f_c	$\beta/\bar{\nu}$	$\gamma/\bar{\nu}$	$\bar{\nu}$	τ
Rnd	0.8	1/3	1/3	3	2.5
ID	0.4652(7)	0.320(4)	0.354(5)	2.72(5)	2.50(2) [2.48(2)]
RD	0.3401(2)	0.307(3)	0.377(7)	2.59(7)	2.43(3) [2.45(2)]
IB	0.558(1)	0.340(3)	0.334(5)	2.8(2)	2.52(2) [2.50(2)]
RB	0.2984(2)	0.10(1)	0.89(2)	1.50(5)	– [2.1(2)]

FIG. 4. Size of the second cluster S_2N as a function of the fraction of nodes removed f for the four attack strategies studied. As it can be seen, this quantity peaks in the neighborhood of the percolation threshold (dashed vertical line). The color code and number of realizations are the same as in Fig. 3. The insets show the collapse of the curves using the scaling ansatz given by Eq. (9), with the parameters given in Table I. (a) ID; (b) RD; (c) IB; (d) RB.

become sharper as N increases, particularly in the case of RB attack. The curves of each panel can be collapsed on both sides of the transition (see insets) using the scaling relation of Eq. (9). The exponents $\beta/\bar{\nu}$ and $\bar{\nu}$ used to collapse the curves corresponding to each attack, which were estimated using the methods described below, are compiled in Table I.

For the four attacks, it can be observed that all the curves collapse very well to a master curve in the proximity of the percolation threshold, confirming that the scaling relations of Eq. (9) hold.

In Figs. 4 and 5, the size of the second largest cluster S_2N and the susceptibility $\langle s \rangle$ are shown. These quantities exhibit a peak close to the percolation threshold, which increases in magnitude with the system size. In the same way as with the order parameter, the curves can be scaled using Eqs. (9) and (10). The corresponding insets show that the collapses are good, thus confirming the validity of the scaling assumptions.

We focus now on the estimation of the critical exponents. By evaluating Eq. (10) at $f = f_c$, we have $\langle s \rangle(f_c, N) \sim N^{\gamma/\bar{\nu}}$, so a log-log plot of $\langle s \rangle$ vs N at the percolation threshold should give a straight line with slope $\gamma/\bar{\nu}$. Thus the ratio between these two exponents can be computed directly using a linear fit. The main drawback of this method is that the percolation threshold must be known beforehand. As we only have an estimation for f_c, this method will propagate the uncertainty associated with that estimation. To avoid this, instead of computing the average cluster size at the percolation threshold, we compute the value at the peak of this measure performing the scaling using these values. We recall that, for sufficiently large system sizes, the scaling of the peaks is the same as the scaling at the percolation threshold [38].

In Fig. 6, we show the corresponding scaling for each of the four attack strategies implemented. In all cases, the linear relation in the log-log scale is very clear. The estimated ratios
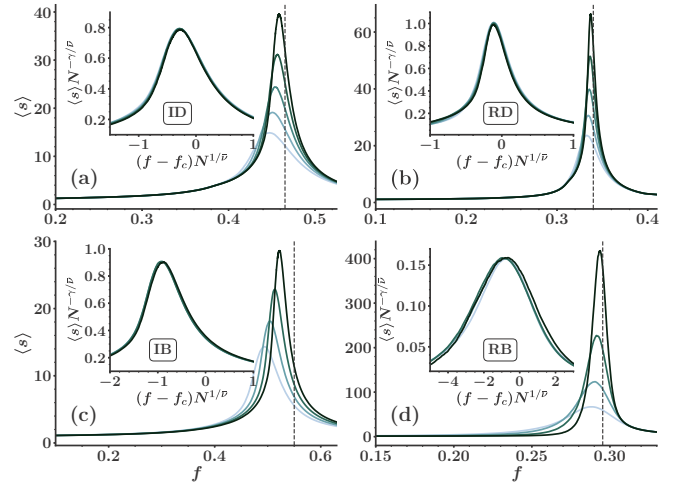
FIG. 5. Susceptibility $\langle s \rangle$ as a function of the fraction of nodes removed f for the four attack strategies studied. As it happens with the size of the second cluster, this quantity also peaks near the percolation threshold. The insets show the collapse of the curves using the scaling ansatz given by Eq. (10), with the parameters given in Table I. The color code and number of realizations are the same as in Fig. 3. (a) ID; (b) RD; (c) IB; (d) RB.

between the critical exponents are shown in the figure and summarized in Table I. In a similar way, we note that the size of the second largest cluster S_2N also peaks near the transition. According to Eq. (9), this quantity scales as $S_2N \sim N^{1-\beta/\bar{\nu}}$ near the critical point, so the ratio $\beta/\bar{\nu}$ can be inferred from the scaling of such peaks. Figure 6 also shows the values of the peaks and the corresponding linear fit. The estimated ratios are summarized, as before, in Table I.

As a consistency check, we note that the estimated exponents satisfy Eq. (6). The values obtained are 0.99(2) for ID, 0.99(2) for RD, 1.01(2) for IB, and 1.09(4) for RB.
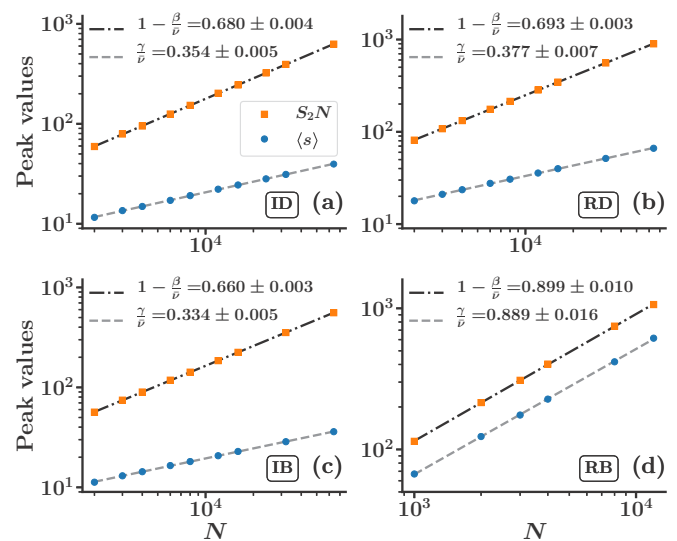

FIG. 6. Scaling of the peaks of S_2N and $\langle s \rangle$ for the four attack strategies. The markers represent the value at the peak, after averaging over N_s realizations. Dashed lines correspond to a linear fit of the points using least squares on a log-log scale. (a) ID, $N_s = 2 \times 10^4$; (b) RD, $N_s = 2 \times 10^4$; (c) IB, $N_s = 2 \times 10^4$; (d) RB, $N_s = 5 \times 10^3$.

To get the full characterization of each transition, it remains to compute the exponent $\bar{\nu}$. In order to do this, we define $G(f, N) = -\partial \log S_1(f, N)/\partial f$ and use Eq. (9) for $i = 1$, from where we have

$$G(f, N) \sim -\frac{d \log \tilde{S}_1[(f - f_c)N^{1/\bar{\nu}}]}{df}$$

$$\sim N^{1/\bar{\nu}}\tilde{G}[(f - f_c)N^{1/\bar{\nu}}], \qquad (12)$$

where $\tilde{G}(x) = -\tilde{S}_1'(x)/\tilde{S}_1(x)$. Then, the function G has a similar scaling than the order parameter and the susceptibility. As the order parameter has an inflexion point close to the percolation threshold, then G has a peak at that point. In the same way as it happens with the susceptibility and the second cluster, it is expected that the peaks scale as a power law, this time, with an associated exponent $1/\bar{\nu}$. Then, we can perform a similar analysis as before and plot G versus N, where we should see a linear relation in a log-log scale. This approach comes with the following caveat. In general, taking the numerical derivative of a noisy signal tends to amplify the noise. Our case is not an exception, as it can be seen in Fig. 7. The gray curves correspond to the numerical derivative computed using five-point finite differences over the average of 2×10^4 realizations (ID, RD, and IB) and 5×10^3 simulations (RB). We can see that the noise is amplified and that it increases with the system size. To overcome this problem, we employed a regularization method, described in [39], with which smoother curves can be obtained (colored curves). The right panels of Fig. 7 show the scaling of the peaks, computed from the regularized derivative. As it can be seen from the linear regressions, the scaling hypothesis is satisfied. The estimated values for the exponent of the correlation length are $\bar{\nu}^{(\text{ID})} = 2.72(5)$, $\bar{\nu}^{(\text{RD})} = 2.59(7)$, $\bar{\nu}^{(\text{IB})} = 2.8(2)$, and $\bar{\nu}^{(\text{RB})} = 1.50(5)$.

C. Cluster size distribution

As it was previously explained, second-order percolation transitions exhibit a power-law cluster size distribution at the critical point given by Eq. (4). In Fig. 8, we show that this is indeed the case for the two degree-based attacks and the initial betweenness attack. The exponents of the respective power laws—which were measured directly from $n(s)$ using a linear fit in logarithmic scale—are in agreement with the scaling relation given by Eq. (5) and are consistent, considering uncertainties, with the value $\tau = 2.5$ correspondent to standard percolation (see Table I). The case of recalculated betweenness deserves special consideration since it departs from the mean-field universality class as we point out below. Although a power-law decaying can be seen for small cluster sizes, the distribution shows a hump at higher values, departing from the expected behavior. In a similar manner to what happens with the abrupt drop in the order parameter near the transition, this behavior could be indicating a first-order phase transition. Nevertheless, it is worth noting that similar effects have been observed in other continuous transitions in the context of explosive percolation models [1,40]. Here we argue that the hump is due to a finite-size transient effect and that it must disappear for larger system sizes. Using a heuristic argument similar to that of Ref. [1], we can estimate a crossover size N^*,
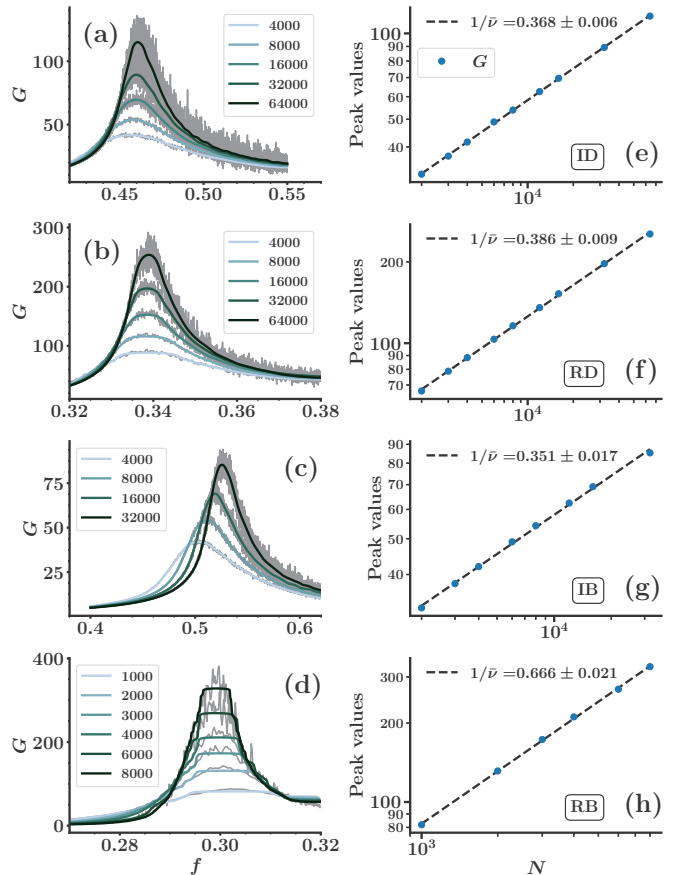

FIG. 7. (a)–(d) Derivative of the logarithm of the order parameter as a function of the fraction of nodes removed. The gray curves correspond to a five-point numerical derivative and the colored curves to the derivatives computed using the regularization method described in [39]. Both methods were applied over averages using 2×10^4 simulations (ID, RD, and IB) and 5×10^3 simulations (RB). (e)–(h) Scaling of the peaks of the curves in the left. Dashed lines correspond to linear fits using least squares. The values obtained for the critical exponent of the correlation length $\bar{\nu}$ are summarized in Table I.

where the system becomes large enough so that realizations converge to the asymptotic limiting behavior. Let $\Delta S_{\max}$ be the greatest jump for the order parameter after removing a node in a single realization. The variation in the control parameter f in this single step is $\Delta f = 1/N$. Assuming that this jump occurs at f_c and using the scaling of the order parameter, we can roughly state that $\Delta S_{\max} \sim \Delta f^{-\beta} = N^{\beta}$. Now, we define N^* as the system size for which the greatest jump in the giant component is about 10%. Thus $N^* \sim 10^{1/\beta}$. For the RB attack, $\beta \sim 0.15$ yielding $N^* \sim 10^6$. As the results presented in Fig. 8 correspond to $N = 16000$, we are still under the crossover size, which might explain the deviation from the power law.

III. DISCUSSION

Table I summarizes the main results of this work, providing a characterization of the percolation transitions produced by the four attack strategies studied. From the perspective of
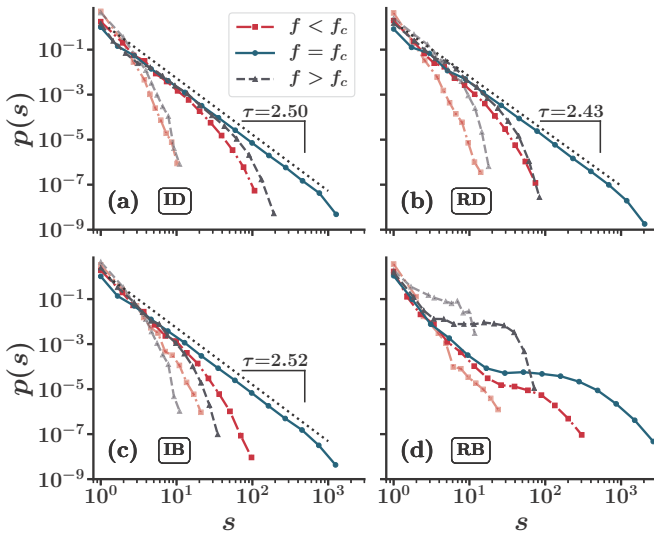
FIG. 8. Cluster size distribution $p(s) = n(s)/\sum'_s n(s)$ for each attack strategy. Dotted dashed red curves correspond to the subcritical region $f < f_c$, dashed gray curves to the supercritical region $f > f_c$, and solid blue lines to the critical value $f = f_c$. For ID, RD, and IB, the plots are consistent with Eq. (4), showing a power-law distribution at the critical point (with a gentle decay at the tail due to finite-size effects) and an exponential decay for other values of f. RB deviates from the standard behavior, showing a hump for middle values of s. The dotted black curves are power laws fitted from the binned data, and their slopes are summarized in Table I. The distributions were computed averaging 10^3 networks. (a) ID, $N = 64000$; (b) RD, $N = 64000$; (c) IB, $N = 64000$; (d) RB, $N = 16000$.

the network dismantling problem, the relevant magnitude is the percolation threshold, which quantifies the strength of each attack. Our results not only confirm that the recomputed versions of the attacks perform better than their initial counterparts, which has been previously shown in the literature [12–14], but also allows us to quantify the amount of improvement that can be achieved by recomputing node centrality at each removal step. If we compare the two degree-based attacks, the difference between their percolation thresholds is around ~ 0.12. For the betweenness-based attacks, the improvement is ~ 0.26. As we see, the difference is greater in the latter case and the reason for this can be attributed to the global nature of the betweenness centrality, in contrast to the locality of the degree.

From the point of view of critical phenomena, the critical exponents are the most relevant measures as they determine the universality class of the transition. Our results show that the two initial attacks have exponents that are consistent or close to the ones corresponding to random percolation. Besides, the scaling relations given by Eqs. (5) and (6) are satisfied within uncertainty. The case of recalculated degree is similar in the sense that it also satisfies the scaling relations, but seems to differ in some of the exponents. The significance of the difference is not clear, however, and in consequence, it is unclear if the attack belongs or not to the same universality class than the previous cases [41]. We note that in a previous work by Norrenbrock *et al.* [42], the authors claim that a RD

attack over two-dimensional proximity graphs has the same exponents as random percolation on a square lattice.

Lastly, the recalculated version of the betweenness-based attack is qualitatively different from the rest of the attacks. The critical exponents are different from the mean-field values and the component size distribution does not exhibit a power-law decay for the system sizes studied. For its characteristics, this transition could be included in the framework of explosive percolation transitions [26,33]. Explosive transitions can be either continuous, with a steep derivative of the order parameter near the percolation threshold, or discontinuous, depending on the underlying process. Given that these transitions are usually characterized by a large crossover size, the order of the transition can be hard to determine. As it has been extensively discussed in recent reviews [1,26], in some cases the transition seems continuous for finite-size systems but becomes discontinuous for large enough systems. In other cases, the opposite occurs. Moreover, there are transitions where both discontinuity and criticality coexist. Based on our results, we can safely say that RB has critical behavior and that it does not belong to the random percolation universality class. On the other hand, we cannot determine the order of the transition from our methods, unless larger systems are studied, which seems unlikely in the short time given the computational complexity associated with the computation of betweenness.

IV. CONCLUSIONS

We have studied the percolation transitions induced by four dismantling strategies based on centrality measures over Erdős-Rényi networks. By performing a systematic finite-size scaling analysis, we have obtained both the percolation thresholds and the critical exponents that characterize the universality class of the transitions. By computing the percolation thresholds, we were able to verify and quantify the intuitive idea that the attack strategies become more effective when node centrality is updated after each removal step. In particular, we show that keeping updated information of node centrality can even modify qualitatively the percolation process, changing its universality class.

From a dismantling point of view, recalculated betweenness is the most efficient attack, as it is the one exhibiting the lowest percolation threshold. In fact, its performance is comparable to the most effective methods to dismantle networks [14,22,23]. Also, the critical exponents of the percolation process associated with this attack are far from trivial, and resemble the behavior observed in explosive percolation transitions [24,31]. At variance with the degree-based attacks where the order parameter gradually decays towards zero, the dismantling with recalculated betweenness proceeds more silently, giving a misleading picture of integrity even at the edge of a catastrophic failure. If we think of infrastructures such as power grids, road networks, or the Internet, it is reasonable to conceive heavy loaded nodes as the most prone to failure, so RB-like damages are possible not only as a targeted attack but as a failure. Other authors have studied the vulnerability of these systems in terms of cascading failures using as a proxy for the loads the betweenness of the nodes [11,21]. From another perspective, our work suggests a

different direction in which networked systems can be assessed in the search of critical vulnerabilities.

ACKNOWLEDGMENTS

[1] R. M. D'Souza and J. Nagler, Anomalous critical and supercritical phenomena in explosive percolation, Nat. Phys. **11**, 531 (2015).

[2] D. Lee, Y. S. Cho, K. I. Goh, D. S. Lee, and B. Kahng, Recent advances of percolation theory in complex networks, J. Korean Phys. Soc. **73**, 152 (2018).

[3] N. Zamponi, E. Zamponi, S. A. Cannas, O. V. Billoni, P. R. Helguera, and D. R. Chialvo, Mitochondrial network complexity emerges from fission/fusion dynamics, Sci. Rep. **8**, 363 (2018).

[4] G. Zeng, D. Li, S. Guo, L. Gao, Z. Gao, H. E. Stanley, and S. Havlin, Switch between critical percolation modes in city traffic dynamics, Proc. Natl. Acad. Sci. USA **116**, 23 (2019).

[5] L. Tian, A. Bashan, D. N. Shi, and Y. Y. Liu, Articulation points in complex networks, Nat. Commun. **8**, 1 (2017).

[6] B. R. Da Cunha, J. C. González-Avella, and S. Gonçalves, Fast fragmentation of networks using module-based attacks, PLoS ONE **10**, 11 (2015).

[7] B. Requião da Cunha and S. Gonçalves, Performance of attack strategies on modular networks, J. Complex Networks **5**, 913 (2017).

[8] L. M. Shekhtman, S. Shai, and S. Havlin, Resilience of networks formed of interdependent modular networks, New J. Phys. **17**, 123007 (2015).

[9] L. D. Valdez, P. A. Macri, and L. A. Braunstein, Temporal percolation of the susceptible network in an epidemic spreading, PLoS ONE **7**, 9 (2012).

[10] A. Allard and L. Hébert-Dufresne, Percolation and the Effective Structure of Complex Networks, Phys. Rev. X **9**, 011023 (2018).

[11] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature (London) **464**, 1025 (2010).

[12] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Attack vulnerability of complex networks, Phys. Rev. E **65**, 056109 (2002).

[13] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, Attack robustness and centrality of complex networks, PLoS ONE **8**, e59613 (2013).

[14] S. Wandelt, X. Sun, D. Feng, M. Zanin, and S. Havlin, A comparative analysis of approaches to network-dismantling, Sci. Rep. **8**, 13513 (2018).

[15] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Network Robustness and Fragility: Percolation on Random Graphs, Phys. Rev. Lett. **85**, 5468 (2000).

[16] R. Albert, H. Jeong, and A.-L. Barabási, Error and attack tolerance of complex networks, Lett. Nature **406**, 378 (2000).

[17] R. Cohen, K. Erez, D. ben Avraham, and S. Havlin, Breakdown of the Internet Under Intentional Attack, Phys. Rev. Lett. **86**, 3682 (2001).

[18] P. Crucitti, V. Latora, M. Marchiori, and A. Rapisarda, Error and attack tolerance of complex networks, Physica A **340**, 388 (2004).

[19] R. Albert, I. Albert, and G. L. Nakarado, Structural vulnerability of the North American power grid, Phys. Rev. E **69**, 025103(R) (2004).

[20] Y. Xia, J. Fan, and D. Hill, Cascading failure in Watts Strogatz small-world networks, Physica A **389**, 1281 (2010).

[21] Y. Kornbluth, G. Barach, Y. Tuchman, B. Kadish, G. Cwilich, and S. V. Buldyrev, Network overload due to massive attacks, Phys. Rev. E **97**, 052309 (2018).

[22] A. Braunstein, L. Dall'Asta, G. Semerjian, and L. Zdeborová, Network dismantling, Proc. Natl. Acad. Sci. USA **113**, 12368 (2016).

[23] F. Morone and H. A. Makse, Influence maximization in complex networks through optimal percolation, Nature (London) **524**, 65 (2015).

[24] D. Achlioptas, R. M. D'Souza, and J. Spencer, Explosive percolation in random networks, Science **323**, 1453 (2009).

[25] R. A. da Costa, S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Solution of the explosive percolation quest: Scaling functions and critical exponents, Phys. Rev. E **90**, 022145 (2014).

[26] R. M. D'Souza, J. Gómez-Gardeñes, J. Nagler, and A. Arenas, Explosive phenomena in complex networks, Adv. Phys. **68**, 123 (2019).

[27] L. C. Freeman, A set of measures of centrality based on betweenness, Sociometry **40**, 35 (1977).

[28] U. Brandes, A faster algorithm for betweenness centrality*, J. Math. Soc. **25**, 163 (2001).

[29] D. Stauffer and A. Aharony, *Introduction to Percolation Theory*, 2nd ed. (Taylor & Francis, London, 1994).

[30] J. G. Brankov, *Introduction to Finite-Size Scaling (Leuven Notes In Mathematical and Theoretical Physics; Series A: Mathematical Physics)* (Cornell University Press, Ithaca, 1996).

[31] S. Fortunato and F. Radicchi, Explosive percolation in graphs, J. Phys.: Conf. Ser. **297**, 012009 (2011).

[32] R. Albert and A.-L. Barabási, Statistical mechanics of complex networks, Rev. Mod. Phys. **74**, 47 (2002).

[33] S. Boccaletti, J. Almendral, S. Guan, I. Leyva, Z. Liu, I. Sendiña-Nadal, Z. Wang, and Y. Zou, Explosive transitions in complex networks structure and dynamics: Percolation and synchronization, Phys. Rep. **660**, 1 (2016).

[34] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Resilience of the Internet to Random Breakdowns, Phys. Rev. Lett. **85**, 4626 (2000).

[35] Y. S. Cho, S. W. Kim, J. D. Noh, B. Kahng, and D. Kim, Finite-size scaling theory for explosive percolation transitions, Phys. Rev. E **82**, 042102 (2010).

[36] Y. Zhu and X. Chen, Finite size scaling theory for percolation phase transition, arXiv:1710.02957 [cond-mat.stat-mech] (2017).

[37] F. Radicchi and S. Fortunato, Explosive Percolation in Scale-Free Networks, Phys. Rev. Lett. **103**, 168701 (2009).

[38] L. S. Ramirez, P. M. Centres, and A. J. Ramirez-Pastor, Standard and inverse bond percolation of straight rigid rods on square lattices, Phys. Rev. E **97**, 042113 (2018).

[39] R. Chartrand, Numerical differentiation of noisy, nonsmooth data, ISRN Appl. Math. **2011**, 1 (2011).

[40] W. Chen, Z. Zheng, and R. M. D'Souza, Deriving an underlying mechanism for discontinuous percolation, Europhys. Lett. **100**, 66006 (2012).

[41] Recently, Ref. [43] has been uploaded to the arXiv, where the authors claim that this attack does belong to the mean-field universality class.

[42] C. Norrenbrock, O. Melchert, and A. K. Hartmann, Fragmentation properties of two-dimensional proximity graphs considering random failures and targeted attacks, Phys. Rev. E **94**, 062125 (2016).

[43] J.-H. Kim, S.-J. Kim, and K. I. Goh, Critical behaviors of high-degree adaptive and collective-influence percolation, arXiv:1911.08421 [physics.soc-ph].