Chaos

Adversarial attack on BC classification for scale-free networks

Cite as: Chaos **30**, 083102 (2020); https://doi.org/10.1063/5.0003707
Submitted: 05 February 2020 . Accepted: 13 July 2020 . Published Online: 03 August 2020

Qi Xuan, Yalu Shan, Jinhuan Wang, Zhongyuan Ruan, and Guanrong Chen

Adversarial attack on BC classification for scale-free networks

Cite as: Chaos **30**, 083102 (2020); doi: 10.1063/5.0003707
Submitted: 5 February 2020 · Accepted: 13 July 2020 ·
Published Online: 3 August 2020

Qi Xuan,[1,2,a] Yalu Shan,[1,2,b] Jinhuan Wang,[1,2,c] Zhongyuan Ruan,[1,2,d] and Guanrong Chen[3,e]

AFFILIATIONS

[1]Institute of Cyberspace Security, Zhejiang University of Technology, Hangzhou 310023, China
[2]College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China
[3]Department of Electrical Engineering, City University of Hong Kong, Hong Kong, China

[a]**Electronic mail:** xuanqi@zjut.edu.cn
[b]**Electronic mail:** 1223071127@qq.com
[c]**Electronic mail:** jinhuanwang@zjut.edu.cn
[d]**Author to whom correspondence should be addressed:** zyruan@zjut.edu.cn
[e]**Electronic mail:** eegchen@cityu.edu.hk

ABSTRACT

Adversarial attacks have been alerting the artificial intelligence community recently since many machine learning algorithms were found vulnerable to malicious attacks. This paper studies adversarial attacks on Broido and Clauset classification for scale-free networks to test its robustness in terms of statistical measures. In addition to the well-known random link rewiring (RLR) attack, two heuristic attacks are formulated and simulated: degree-addition-based link rewiring (DALR) and degree-interval-based link rewiring (DILR). These three strategies are applied to attack a number of strong scale-free networks of various sizes generated from the Barabási–Albert model and the uncorrelated configuration model. It is found that both DALR and DILR are more effective than RLR in the sense that rewiring a smaller number of links can succeed in the same attack. However, DILR is as concealed as RLR in the sense that they both are introducing a relatively small change on several typical structural properties, such as the average shortest path-length, the average clustering coefficient, the average diagonal distance, and the Kolmogorov–Smirnov test of the degree distribution. The results of this paper suggest that to classify a network to be scale-free, one has to be very careful from the viewpoint of adversarial attack effects.

Scale-free and small-world properties are considered as the two most important in real-world networks, which may largely influence many dynamical processes, such as epidemic spreading, information cascading, and synchronization. Quite recently, Broido and Clauset (BC) proposed a classification method to estimate the strength of the scale-free attribute of a network and concluded that scale-free networks are rare in reality. Their work has attracted much attention in the network science community and triggered wide discussions. The current paper focuses on testing the robustness of this scale-free network classification method and meanwhile proposes two heuristic adversarial attack strategies, namely, degree-addition-based link rewiring (DALR) and degree-interval-based link rewiring (DILR). The experiments show their effectiveness in misleading the BC classification by only rewiring a small number of links, indicating that BC classification could be quite vulnerable to purposefully designed noises. We hope our study may provide a different perspective to the argument on scale-free networks and suggest to test the robustness of statistical classifications derived from real-world data against various adversarial attacks.

I. INTRODUCTION

Scale-free networks are ubiquitous in nature and society, from email networks[1] to cell networks,[2] from World-Wide Web[3] to social networks,[4] and beyond. In a scale-free network, few nodes have large numbers of connected links, exhibiting remarkable heterogeneity in node degrees. This special feature makes them highly robust against random attacks but extremely vulnerable to targeted attacks, which is known as the *Achilles Heel* effect.

Generally, a network is considered to be scale-free if its degree distribution follows a power-law form, i.e., $p(k) \sim k^{-\alpha}$, where k is the node degree and α is the power-law exponent. Since the influential report on scale-free networks,[5] referred to as the Barabási–Albert (BA) model, there have been a lot of studies,[6,7] especially several key discoveries helped the community understand the origins of the different exponents. The rate-equation based continuum theory, developed by Mendes, Dorogovtsev, Redner, Krapivsky, and many others,[8] helped incorporate into the scale-free model many effects that naturally occur in real-world networks, like the disappearance of nodes, the addition of new links between previously existing nodes, link deletion, aging, and so on.[9] Correspondingly, the studies of how the scale-free structure of networks affects the dynamics (such as epidemic spreading,[10] synchronization,[11,12] and so on) also have drawn a great deal of attention. Researchers found some surprising results based on scale-free networks. For example, it is found that the epidemic threshold is absent in scale-free networks in the thermodynamic limit, and the scale-free networks would lead to the emergence of cooperation, etc. In fact, scale-free networks have been widely used as a substrate in network science nowadays.

Although the scale-free network occupies an important position in network science, the controversy on scale-free has been going on for years. Central to this debate is that the definition of scale-free network is not clear: in some cases, the definition is stricter. For example, it may require that the power-law exponent satisfies $\alpha \in (2, 3)$ or its generation mechanism has a preferential attachment operation.[13] In some other cases, the definition is broader. For example, it may only require the upper tail of the degree distribution curve to satisfy the power-law form,[14] or its log–log curve is nearly straight.

The discussions on the definition of a scale-free network have attracted considerable attention since early 2018 when Broido and Clauset[15] proposed a classification method to estimate the strength of the scale-free attribute of a network. They tested nearly 1000 real-world networks and concluded that scale-free networks are rare. Network scientists agree, by and large, that the BC classification's analysis is statistically sound. Critics of the scale-free viewpoint object that terms like "scale-free" and "heavy-tailed" are bandied about in the network science literature in such vague and inconsistent ways.[16] It is necessary to propose a classification method of scale-free networks. Moreover, these results undermine the universality of scale-free networks.[15] If this conclusion is proved to be correct, then many previous studies on scale-free networks may be re-examined because the networks they use are not scale-free at all. In summary, the BC classification has an important impact on the development of scale-free networks. We should seriously explore the rationality of the BC classification.

Supporters of the scale-free viewpoint argue that scale-free is intended as an idealized model. Therefore, they questioned the BC classification on real-world networks. Barabási[9] believes that there are some deficiencies in BC classification: in real-world networks, if the scale-free is present, the power-law tends to coexist with some corrective function, expecting power-laws with exponential cutoffs, stretched exponentials, logarithmic corrections to the power law, and so on. Moreover, Barabási pointed out that the BC classification has something wrong on the synthesis networks because there is no synthesis network that can be considered as the strongest scale-free network in Ref. 15. Coincidentally, Voitalov *et al.*[17] also pointed out that if the fitted model is a pure power-law model, there is no question that scale-free networks are rare, but in reality, due to the existence of noise, sampling, or other processing factors, it is not possible to obtain a pure power-law distribution. In this paper, we verify the BC classification from a different perspective: testing the BC classification under purposefully designed noises, i.e., under adversarial attack, which is frequently used in the area of AI.

Noise plays an important role in many aspects of data analysis. Since deep learning is widely used in computer vision,[18,19] there are a number of studies on algorithm robustness.[20–23] It was found that changing a few pixels in an image could make the classification result totally wrong or different. The reason is that the feature vector of the image will change when a pixel is modified, which can fool many deep learning algorithms. For example, Su *et al.*[21] only changed one pixel in an image, and they were able to destroy many intrinsic properties of the image and fool a deep neural network. Besides, there are many other ways to add such disturbances to an image, e.g., Fast Gradient Sign Method (FGSM),[24] Iterative Least-likely Class Method (ILCM),[25] DEEPFOOL,[22] and so on. Most of these methods can only generate a specific disturbance for a specific image; instead, Moosavi-Dezfooli *et al.*[26] created general perturbations for a bunch of images, making the situations even worse, since such disturbances are not easily identifiable by humans.

Besides computer vision, in the area of network science, it was also found that simple purposeful modifications to an original network, i.e., by rewiring links, adding/deleting nodes, or changing nodes' attributes, can significantly change the network properties and thus greatly disturb the graph algorithms.[27] Recently, a number of strategies were proposed to attack link prediction,[28,29] node classification,[30] and community detection.[31] For instance, Yu *et al.*[32] proposed heuristic and evolutionary algorithms to protect targeted links from link-prediction-based attacks. Zügner *et al.*[33] considered attacking node classification and introduced NETTACK based on a graph convolutional network (GCN) to generate adversarial attack iteratively. Chen *et al.*[31] used a genetic algorithm (GA)-based Q-attack to destroy the community structure of a network, where the modularity Q is used to design the fitness function.

On the other hand, p-value is dominant in statistical analysis, which, however, has been questioned before.[34] Today, the p-value measure has been re-examined and advanced to a new climax.[35] More than 800 reports pointed out that the sample size has a great impact on the p-value. By adding or subtracting some data, which can be considered as noise, one will get a different result compared with the original one, which leads to a conclusion that two studies conflict because one had a statistically significant result and the other did not.[35]

The reality is, unfortunately, what you see from the data may not mean what they really are. In other words, the algorithms and models developed based on real-world data could be vulnerable to tiny noise and purposefully designed noise-like perturbations. Therefore, the robustness of machine learning algorithms attracts more and more attention from the Artificial Intelligence (AI) community. The robustness of many classifications, especially those based on data, has to be examined to ensure that they are reliable.

Motivated by the above discussions, in this paper, a new type of *adversarial attack* is introduced to the robustness of BC classification on *scale-free* networks. In reality, it is common to see

that many systems are frequently perturbated by such "man-made" noises. Here are two examples: (1) At the early stage of an epidemic outbreak, a few people with awareness in the social network may actively cut links with some "central" nodes who have a high risk of infection.[36] (2) In online social networks, some newly created malicious accounts may link to nodes with large degrees to spread a certain piece of false information.[37,38] These kinds of changes in networks can be regarded as purposeful perturbations. We here try to check whether the BC classification is robust against such purposeful perturbations. If it fails, for example, it would be dangerous to apply the BC classification to the networks. Specifically, three attack strategies are used to evaluate the robustness of the classification method proposed for scale-free networks.[15] To be convincing, the Barabási–Albert (BA) model and the uncorrelated configuration model (UCM) are used to generate 100 *strong* scale-free networks of different sizes for testing the attacks in experiments by rewiring some links of these networks until the Broido–Clauset (BC)[15] classification goes wrong. The results show that the BC classification can be easily fooled by rewiring only a small fraction of links.

The main contributions of this paper are summarized as follows.

- *Adversarial attack* is introduced onto the BC classification of scale-free networks to evaluate its robustness under purposefully designed noise-like perturbations.
- Two heuristic attack strategies, namely, *degree-addition-based link rewiring* (DALR) and *degree-interval-based link rewiring* (DILR), are introduced. Also, several concealment metrics are proposed to measure their effectiveness and concealment.
- It is found that both DALR and DILR are more effective than random link rewiring (RLR), in terms of rewiring fewer links to successfully attack strong scale-free networks, so that the networks become other types. It is also found that DILR is as concealed as RLR in that they both are constructed by introducing a relatively small number of changes on several typical structural properties such as the average shortest path-length, the average clustering coefficient, the average diagonal distance, and the degree distribution. Therefore, the results of this paper suggest that to classify a network to be scale-free, one has to be very careful from the viewpoint of adversarial attack effects.

The rest of the paper is organized as follows. The BC classification of scale-free networks is introduced in Sec. II. Three adversarial attack strategies are proposed in Sec. III. Some metrics for attack effectiveness and concealment are discussed with experimental results reported in Sec. IV. Conclusions are drawn in Sec. V.

II. CLASSIFICATION OF SCALE-FREE NETWORKS

Here, the classification of scale-free networks proposed by Broido and Clauset[15] is reviewed, which is referred to as the BC classification below.

1. *Preprocessing the real-world network data.* Common analysis typically relies on the *scale-free hypothesis* to determine whether a network is scale-free or not. This hypothesis states that a network is scale-free if its degree distribution follows a power-law form, where only the information of a node degree is taken into account, while real-world networks carry many irrelevant attributes such as link weights, connection directions, etc., which make it inconvenient to estimate the strength of the scale-free attribute. Thus, the BC classification suggests to first convert the original network to a set of simple graphs, where one can apply the scale-free hypothesis to each graph. In this way, one can obtain several degree sequences. For example, from a directed network, one can get an in-degree sequence and an out-degree sequence (see Fig. 1). To that end, one can put all the degree sequences in a set, S.
2. *Estimating the strength of a scale-free attribute of each degree sequence.* Several indicators are used in BC classification to estimate the strength of a scale-free attribute for a given network, which are listed in Table I, where R is the newly proposed one to evaluate the best fit model.
3. *Classifying the networks.* According to the above two steps, one can determine the strength of the scale-free attribute of a network based on which the real networks in examination

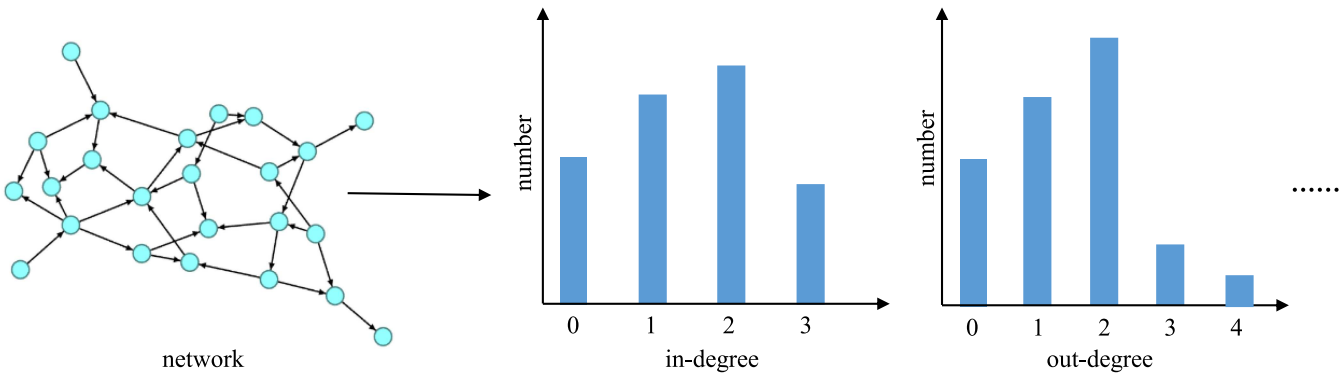

FIG. 1. Preprocessing of a real-world network under the BC classification framework. Taking a directed network as an example, the directed attribute is removed, and both in-degree and out-degree sequences are obtained.

TABLE I. Indicators for the scale-free attribute in BC classification.

Indicators	Description
α	Power-law exponent obtained by fitting a power-law degree distribution model
n_{tail}	Number of tail nodes used for fitting
p	$p \geq 0.1$: Accept the scale-free hypothesis $p < 0.1$: Reject the scale-free hypothesis.
R	$R > 0$: The power-law model is much in favor $R = 0$: The data do not permit a distinction between (power-law or alternative) models $R < 0$: The alternative model (such as the exponential model) is much in favor

were divided into six categories: *strongest*, *strong*, *weak*, *weakest*, *super-weak*, and *non-scale-free*, as shown in Fig. 2. It can be seen that the strongest, strong, weak, and weakest classes are nested, indicating that the strength of the scale-free attribute becomes weaker gradually. The super-weak class indicates that the networks are extremely weak in a scale-free attribute, which only requires that the optimal distribution is in a power-law form. Networks that do not fall into the above five categories are considered as non-scale-free networks.

Broido and Clauset[15] analyzed nearly 1000 networks in different domains, and they found that only a small number of them can be considered as strongest or strong scale-free networks; even the undirected and unweighted networks (simple networks) generated by the BA model do not entirely belong to the strong category. Thus, they concluded that scale-free networks are rare. This classification method has attracted much attention in the network science community and triggered wide discussions recently.[9,16,17,39]

III. METHOD

In a computer vision simulation, as an adversarial attack example, tiny perturbations are added into a panda picture. It is very difficult for one to find differences between the attacked picture and the original one. This surprisingly can make the classification algorithm misjudge it to be a gibbon picture with a probability of 99.3%.[24]

In this paper, the adversarial attack is applied to fool the BC classification introduced in Sec. II. Specifically, by rewiring a few links in the network to alter the values of the indicators, namely, making the indicators exceed the limit of the original category, the attack can make the BC classification results go wrong. According to the BC classification algorithm, the difference between the strong category and the weak category is determined by the power-law exponent α and the indicator R in Table I, and the difference between the weak and weakest categories is determined by n_{tail}, the number of fitting nodes. It is emphasized that the power-law exponent α plays a more important role than the indicator R on determining the strong category.[15] Therefore, in this paper, the adversarial attack strategy is designed based on the measures of both the power-law exponent α and the number of fitting nodes n_{tail}.

A network is represented by a graph $G = (V, E)$, where V and E represent the sets of nodes and links in the network, respectively. Let Ω represent the set of links in the fully connected network with the same set of nodes V. Note that E is a part of set Ω. Define $N = \Omega - E$ as the set of links in the complementary network of G, namely, those in the fully connected network but are not in the network G.

A. Random link rewiring

In the random link rewiring (RLR) scheme, one first randomly selects a link $l_{delete} \in E$ to delete and a link $l_{add} \in N$ to add at each step time so as to balance the number of links in the network. After

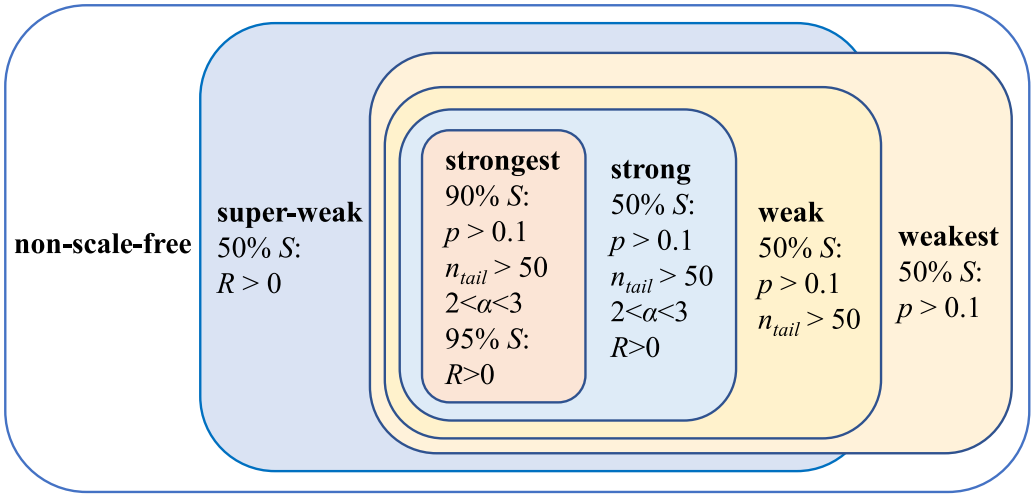

FIG. 2. The real-world networks in examination are classified into six categories:[15] strongest, strong, weak, weakest, super-weak, and non-scale-free.

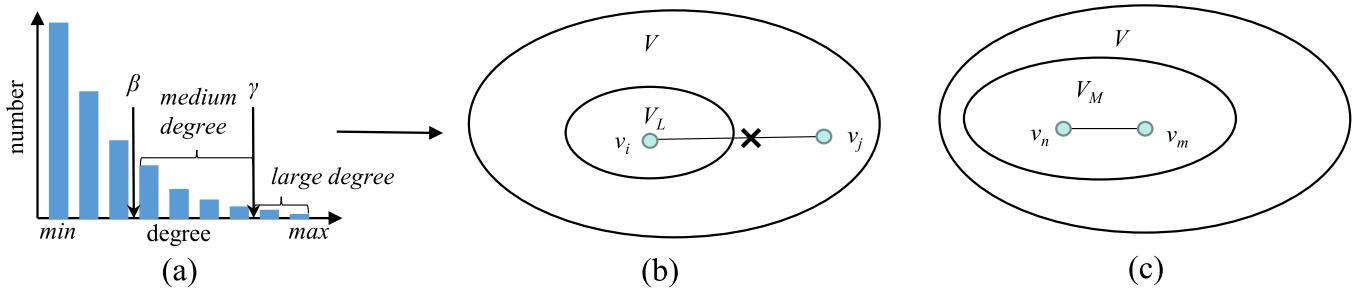

FIG. 3. Illustration of the DILR attack strategy. (a) Determine the set of large-degree nodes, V_L, and the set of medium-degree nodes, V_M, according to the degree sequence. (b) Delete the link between two connected hub nodes (note that, here, the node v_j has the largest degree among all the neighbors of v_i; therefore, it could be either in or not in V_L). (c) Add a link between two unconnected nodes of medium degrees.

an attack, the set E and N become E' and N', respectively,

$$E' = E - l_{delete} + l_{add}, \tag{1}$$

$$N' = N + l_{delete} - l_{add}. \tag{2}$$

Thus, one gets a new *adversarial network* $G' = (V, E')$.

B. Degree based link rewiring

One of the prominent properties of scale-free networks is that there exist a few nodes with extremely large degrees called hubs. These hubs are key to the robustness of the networks—they make the scale-free networks be highly tolerant to random attacks while extremely vulnerable to targeted attacks,[40] measured by the connectivity or the average shortest path-length of the network. Moreover, they play an important role in some dynamical processes taking place on the networks, such as epidemic spreading,[41,42] information cascading,[43] and synchronization.[11,12]

1. Degree-addition-based link rewiring (DALR)

Roughly divide the links in a scale-free network into three categories: hub–hub links (links connecting two hubs), hub–normal links (links connecting one hub and one normal node), and normal–normal links (links connecting two normal nodes). Then, DALR is designed based on the following two operators.

- *Deleting a hub–hub link.* Since the number of hub–hub links in a scale-free network is generally quite small, this condition can be relaxed as follows: first, design an indicator $d_{(i+j)}$ to measure the degree of node pairs,

$$d_{(i+j)} = d_i + d_j, \tag{3}$$

  where d_i and d_j represent the degrees of nodes v_i and v_j, respectively. Then, sort the links according to their values of $d_{(i+j)}$, from large to small. The link with the highest ranking will be chosen to remove.
- *Adding a normal–normal link.* In order to weaken the scale-free attribute without changing the network density, add a normal–normal link since this operation can weaken the heterogeneity of the network. Specifically, the nodes are sorted according to their degree from small to large, and the link between the pair of unconnected nodes with the smallest sum of degrees is chosen to connect together.

2. Degree-interval-based link rewiring (DILR)

The main indicators of strong and weak categories are the power-law index α and the number of fitting nodes, n_{tail}, which are determined by the fitting process. Divide the node distribution into two parts according to the fitting process: the tail of the distribution used for fitting and the others for another purpose. As is well known, the power-law index α is determined by the (average) slope of the curve; therefore, if the tail is steeper with the smaller n_{tail}, it will be out of the strong and weak categories much easily.

Based on the above observations, one can roughly divide the nodes into three sets: nodes with large degrees (within $\gamma = 20\%$), nodes with medium degrees (between γ and β, with β varying from 35% to 70%), and nodes with small degrees (the remaining ones), as shown in Fig. 3. Denote V_L and V_M the nodes of large degrees and medium degrees, respectively. Then, the following DILR attack strategy is designed.

- *Deleting a link between two connected hub nodes.* First, select a node $v_i \in V_L$ and then choose $v_j \in N_i$, where N_i is the neighboring set of v_i, such that v_j has the largest degree among all neighbors of v_i. Then, delete the link between v_i and v_j.
- *Adding a link between two unconnected nodes of medium degrees.* Randomly select two unconnected nodes from V_M and add a link between them.

IV. EXPERIMENTAL RESULTS

A. Datasets

There are many models for generating scale-free networks: the BA model,[5] the fitness model,[44] the local-world evolving network models,[45–48] the uncorrelated configuration model (UCM),[49] etc. The BA model is rooted in growth and preferential attachment and can explain the mechanism behind the scale-free attribute of a network. In this paper, the most well-known BA model and the UCM model are adopted to generate simple networks (undirected

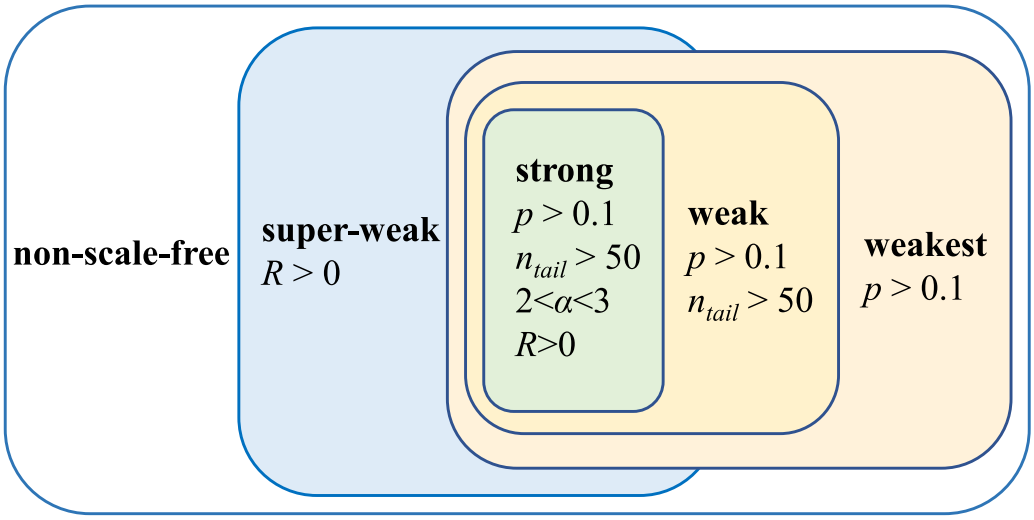

FIG. 4. Classification of simple networks generated by the BA model in terms of the scale-free attribute. Here, strongest and strong categories are merged into one, the strong category, and the other four categories keep the same, as suggested by Broido and Clauset.[15]

and unweighted networks). All the generated networks are simple, and each simple network only has one degree sequence. Figure 2 shows that the main difference between the strong category and the strongest category is the number of graphs (degree sequences) that satisfies the requirements. Therefore, there will be no difference between the strong category and the strongest category for a simple network, and we combine the two categories into one. In other words, only the following five categories are considered here: *strong*, *weak*, *weakest*, *super-weak*, and *non-scale-free*, where the former three are nested, as shown in Fig. 4. In order to test the robustness of the BC classification method, we attack the networks generated by the BA model and the UCM model of different sizes: $n = 500$, 1000, and 2000, respectively, where n is the number of nodes. For BA model networks, the number of links, m, is set to be $2n$, for simplicity. For UCM model networks, the number of links could vary in each network, and we average the network links of each size: $m = 895$, $m = 1688$, and $m = 3870$, respectively.

In the simulation, 500 networks for each size were generated and then classified. Table II shows the classification results, where it can be seen that most (but not all) of the networks generated by the BA model and the UCM model indeed fall into the strong category regardless of the sizes of the networks. However, there are still some networks that cannot be considered as scale-free networks by the BC classification; specifically, more than 10% of them are considered as super-weak and very few of them are considered as weak. It is worth mentioning that few networks are in the weakest category. For the BA model, we surprisingly find that more networks will be classified into the non-scale-free category as the network size increases, while it is opposite in the UCM model networks.

B. Performance metrics

1. Metric for effectiveness

When attacking a model or a scheme, one always hopes that the attack could successfully fool the object with the lowest cost, e.g., changing the least number of pixels to fool a computer vision model or rewiring the least number of links to fool a link prediction or a node classification algorithm. Here, to measure the effectiveness of different adversarial attack strategies, the smallest fraction of rewired links needed to successfully fool the BC classification method[15] is considered by changing the *strong* category of scale-free

TABLE II. Classification results of the networks generated by the BA model and the UCM model of different sizes. Most but not all of them fall into the strong category.

n	Strong (%)	Weak (%)	Weakest (%)	Super-weak (%)	Non-scale-free (%)
500 (BA)	89.30	0.30	0	10.30	0
1000 (BA)	78	0	0	20.60	1.40
2000 (BA)	73.60	0.20	0	14.60	11.60
500 (UCM)	46.96	10.87	0.43	16.09	25.65
1000 (UCM)	56.47	2.94	0	15.88	24.71
2000 (UCM)	56.32	2.30	0	24.13	17.24

networks to another type. The metric is defined by

$$\Delta M = \frac{m_R}{m}, \tag{4}$$

where m_R is the smallest number of rewired links to realize a successful attack and m is the total number of links in the whole network. If a (strong) scale-free network is still in the strong category after a large perturbation introduced by the attack, i.e., a large fraction of links are rewired, then it is deemed that the classification algorithm is robust or the attack is less effective.

2. Metrics for concealment

Generally, rewiring a network may not only change the scale-free attribute (the objective here), but also change other structural properties of the network. In this sense, defenders may utilize certain structural properties to discover the adversarial attack.

To quantify the concealment of various adversarial attacks, the following four metrics are proposed for measuring the structural changes introduced by an attack.

- *Relative change of the average distance* (ΔL). The average distance, or the shortest path-length, is defined as

$$L = \frac{2}{n(n-1)} \sum_{i \geq j} d_{ij}, \tag{5}$$

where n is the number of nodes and d_{ij} is the shortest path length between nodes v_i and v_j.

The average shortest path-length is one of the most typical global characteristics of a network. Due to the existence of hubs, the average shortest path of a scale-free network is generally shorter than that of a random network.[50] This means that if a network has a strong evidence to be scale-free, its average path-length should always be short.

Here, the focus is on the relative change of L introduced by the attack. Denote by $L_{original}$ and $L_{adversarial}$ the average shortest path-length of the original network and the adversarial network, respectively. Then, the relative change of L is defined as

$$\Delta L = \frac{|L_{adversarial} - L_{original}|}{L_{original}}. \tag{6}$$

- *Relative change of the average clustering coefficient* (ΔC). The clustering coefficient[51] is defined as the ratio of the actual number of links among the neighbors of a node to the maximum possible number of links among the neighbors. The average clustering coefficient of a whole network is defined as

$$C = \frac{1}{n} \sum_{i=1}^{n} \frac{2E_i}{k_i(k_i - 1)}, \tag{7}$$

where k_i is the number of neighbors of the node v_i and E_i is the actual number of links among the neighbors of v_i.

The clustering coefficient, as the most typical local property, reflects how densely the neighbors of a node are connected to each other. In scale-free networks, the probability of having a link between two nodes connecting to the same node is relatively low. As a result, scale-free networks generally have small average clustering coefficients.

Similarly, here, the focus is on the relative change of C introduced by the attack. Denote by $C_{original}$ and $C_{adversarial}$ the average clustering coefficient of the original network and the adversarial network, respectively. Then, the relative change of C is defined as

$$\Delta C = \frac{|C_{adversarial} - C_{original}|}{C_{original}}. \tag{8}$$

- *Relative change of the diagonal distance* (ΔD). The diagonal distance,[52] denoted by D, measures the average distance from the main diagonal of nonzero elements in the adjacency matrix of a graph, which is defined as

$$D = dd(A) = \langle dd \rangle = \frac{1}{n^2} \sum_{(i,j) \in E} dd_{ij}$$
$$= \frac{1}{n^2} \sum_{(i,j) \in E} \frac{x_{ij} \cdot y_{i,j}}{z_{ij}} = \frac{1}{\sqrt{2} \cdot n^2} \sum_{(i,j) \in E} |i - j|, \tag{9}$$

where dd_{ij} is the distance of the elements i and j from the main diagonal of the adjacency matrix A, $x_{ij} = |(i,i) - (i,j)|$, $y_{ij} = |(j,j) - (i,j)|$, $z_{ij} = \sqrt{x_{ij}^2 + y_{ij}^2}$, n is the number of network nodes, and $\langle \cdot \rangle$ is the average operation. It was found[52] that the diagonal distance can be used to detect the dramatic changes in the topology of a network. Here, the relative change of D is used to measure the attack concealment, which is defined as

$$\Delta D = \frac{|D_{adversarial} - D_{original}|}{D_{original}}, \tag{10}$$

where $D_{original}$ and $D_{adversarial}$ are the average diagonal distances of the original network and the adversarial network, respectively.

- *KS test on the degree distribution.* The Kolmogorov–Smirnov (KS) test checks two independent distributions that are similar or different by generating cumulative probability plots for two distributions and finding the distance along the y-axis for the given x values between the two curves. From all the distances calculated for each x value, the maximum distance is searched. This maximum distance or maximum difference is then plugged into a KS probability function to calculate the probability value. The lower the probability value is the less likely the two distributions are similar. Conversely, the higher probability means that the two distributions are more similar.

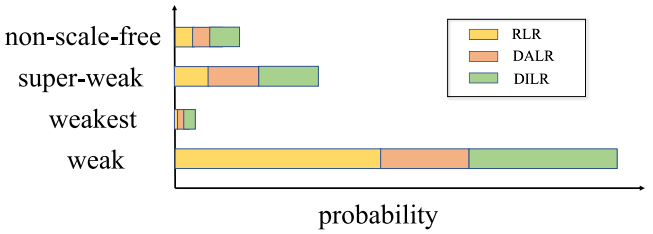

FIG. 5. Probabilities of adversarial networks that belong to different categories. The chart shows the overall results by considering all the cases (three attack strategies on all the networks of different sizes).

The BC classification is mainly based on the degree distribution. Therefore, it is important to test the differences between the degree distributions of the original networks and those of the adversarial networks.

C. Results

In this study, 100 networks were randomly selected from the strong category in the generated networks of each size n to attack, for $n = 500$, 1000, and 2000, respectively.

Note that the most important indicators for distinguishing strong and weak categories are the power-law exponent α and the indicator R in Table I. Therefore, the goal here is to make the power-law exponent α be out of the range of the strong category by using the attack strategies introduced in Sec. III. An attack is repeated until the network does not meet the strong category requirement. Then, the resultant adversarial network is reclassified.

The results show that such an attack not only changes the power-law exponent α, but also changes the indicators p and n_{tail}, which makes the adversarial networks be chanced to other categories. However, the probability of falling into each new category is different. To reduce the contingency of the attack results, each network is attacked 200 times and the mean results are recorded. In the simulation, it was found that 200 times are enough for the probability to converge for the tested networks.

For the DILR attack strategy, there is a question of how to divide the intervals according to the node degree. In general, the degree distribution of a scale-free network satisfies the Pareto principle, which has been widely used in sociology and business management, indicating that for a scale-free network, the hub nodes are concentrated on the top 20% of the degree ranking. For this reason, the γ in the DILR strategy is set to be 20%. However, because it is not clear how to determine the interval of intermediate node degrees, the indicator β is tuned among five different values, 35%, 40%, 50%, 60%, and 70%. The experimental results show that both the probability of a successful attack and the cost of the attack increase as β increases. Considering the balance between the two, the indicator is set as $\beta = 50\%$ in the simulation.

Now, the three attack strategies, RLR, DALR, and DILR, are applied onto the BA *strong* scale-free networks and UCM *strong* scale-free networks of different sizes. An attack will be ended as soon as the adversarial network does not belong to the *strong* category, no matter it is in *weak*, *weakest*, *super-weak*, or *non-scale-free*. The following are three findings.

First, it seems that the probabilities of the adversarial networks (obtained by attacking strong scale-free networks) belonging to different categories are quite different. Overall, by considering all the cases (three attack strategies on the networks of different sizes), the adversarial networks are most likely to be in the weak category (with probability 62.92%) but are most difficult to be in the weakest category (with probability 1.75%), as shown in Fig. 5. By comparison, the adversarial networks are relatively easier to be in the super-weak category, rather than in the non-scale-free category, with properties 23.96% and 11.37%, respectively. This is because, generally, it is quite costly (a large number of links need to be rewired) to make n_{tail} less than 50, especially for those networks of large sizes, where $n_{tail} \leq 50$ is the threshold to define the weakest category. On the contrary, the other three parameters, α, R, and p, are more sensitive to the attacks since they are determined by the overall curve of the degree distribution, especially for α and p. Note that the fractions of adversarial networks in different categories are slightly different by adopting different attack strategies; e.g., most of the adversarial networks in the weak category are generated by RLR, while most of those in the other three categories (weakest, super-weak, non-scale-free) are generated by DILR. However, overall, these strategies are consistent with each other.

Second, the two heuristic attack strategies are much more effective than the random rewiring strategy RLR in the sense that a smaller ΔM is needed to succeed in the attack, while among them, DILR is the most effective one. As shown in Tables III and IV, for RLR, which can be considered as random noise, typically more than 15% links in the BA original networks need to be rewired to succeed in the attack (from strong to weak, weakest, or super-weak) and more than 10% links in the UCM original networks. However, surprisingly, only around 5% links need to be rewired when the network is attacked to become non-scale-free, although such cases are rare (as shown in Fig. 5). This result suggests that the BC classification could be robust against small random noise. More interestingly, when the perturbations are purposefully designed, the BC classification will be quite vulnerable; i.e., only 3.89% links (38.9 in 1000 links on average) need to be rewired if DILR is applied to attack the networks of 500 nodes, much less than the value of 17.30% by RLR. It seems that, as the network size increases, it is more difficult to succeed in an attack; e.g., the fractions of rewired links for both DALR and DILR steadily increase as the network size increases. Even so, the number of rewired links needed by DALR or DILR is only half of those needed by RLR, when the networks have 2000 nodes and 4000 links. By comparison, DILR is generally more effective than DALR; i.e., a smaller number of links are needed to succeed in attack when DILR is applied rather than DALR. There are differences between the two models, and the costs of the attack on BA model networks are much more expensive than those on UCM model networks. On UCM model networks, the cost of DALR is close to that of DILR, but both of them are much lower than tha t of RLR.

Third, the adversarial attack will not change the network structure by too much; i.e., the relative changes of L, C, D, and KS test introduced by DILR are comparable with those introduced by RLR. It is well known that the average shortest path-length L and the average clustering coefficient C are good for characterizing the global and local properties, respectively. On the other hand, the recently proposed diagonal distance D is also a global property useful for detecting the dramatic changes in the topology of a network.[52] Moreover, the degree distribution is the core of the BC classification. First, the relative changes of former three properties are used, i.e., ΔL, ΔC, and ΔD between the original networks and the adversarial networks, to measure if these properties will dramatically change under adversarial attacks. The results are presented in Tables V and VI. It is found that, overall, ΔL introduced by DILR is larger than those introduced by RLR, but much smaller than that introduced by DALR, and that DILR and RLR have comparable ΔC, around 30% for BA model networks and around 10% for UCM model networks, which is only half of that introduced by DALR.

TABLE III. The minimum fractions of rewired links (ΔM) needed for a successful attack, for different attack strategies on BA model networks of different sizes. Here, the symbol "…" means that there is no adversarial network belonging to the *weakest* category when the DALR strategy is applied. The best results are marked in bold for each category.

Network size	Attack strategy	Strong→weak (%)	Strong→weakest (%)	Strong→super-weak (%)	Strong→non-scale-free (%)	Overall (%)
$n = 500$	RLR	17.70	15.60	17.40	5.40	17.30
	DALR	6.40	6.00	6.20	5.40	6.33
	DILR	**3.40**	7.80	**4.10**	**4.00**	**3.89**
$n = 1000$	RLR	17.00	14.91	16.72	4.46	16.19
	DALR	7.56	**9.60**	7.16	7.60	7.68
	DILR	**5.83**	13.08	**4.47**	**3.95**	**5.51**
$n = 2000$	RLR	16.25	**16.38**	16.78	**5.13**	16.07
	DALR	**8.28**	…	7.94	7.60	**8.16**
	DILR	10.35	20.20	**5.50**	6.02	8.71

TABLE IV. The minimum fractions of rewired links (ΔM) needed for a successful attack, for different attack strategies on UCM model networks of different sizes. Here, the symbol "…" means that there is no adversarial network belonging to the *weakest* category when the DALR strategy is applied. The best results are marked in bold for each category.

Network size	Attack strategy (%)	Strong→weak (%)	Strong→weakest (%)	Strong→super-weak (%)	Strong→non-scale-free (%)	Overall (%)
$n = 500$	RLR	4.87	**12.84**	10.61	2.99	7.83
	DALR	**1.34**	…	2.57	**0.80**	**1.57**
	DILR	1.40	…	**2.12**	1.47	1.67
$n = 1000$	RLR	7.66	7.92	16.01	3.59	8.80
	DALR	2.03	…	4.34	**0.70**	2.36
	DILR	**1.97**	**3.92**	**3.29**	1.37	**2.10**
$n = 2000$	RLR	16.23	…	25.25	4.96	15.48
	DALR	**3.26**	…	5.97	3.36	**4.19**
	DILR	27.05	…	**4.01**	**1.83**	10.96

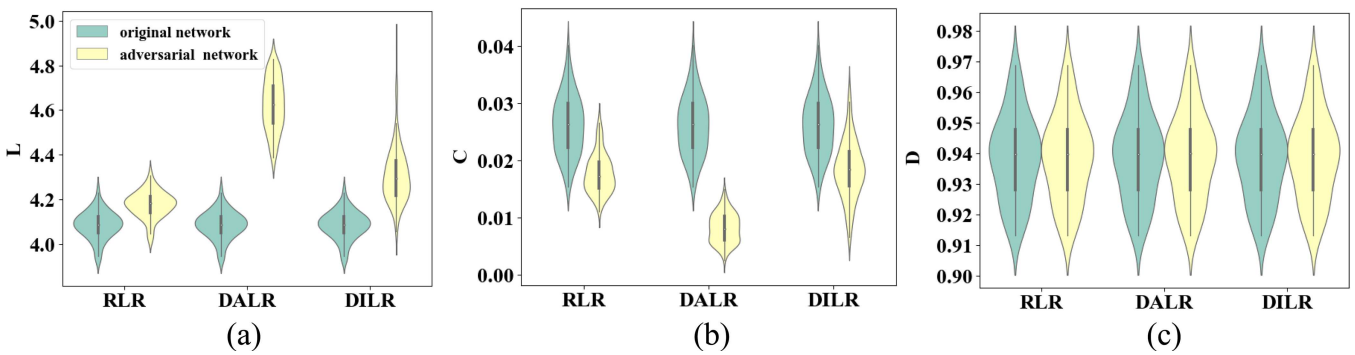

FIG. 6. The violin plots of the three structural properties: (a) L, (b) C, and (c) D, of the networks both before and after the attacks by different strategies.

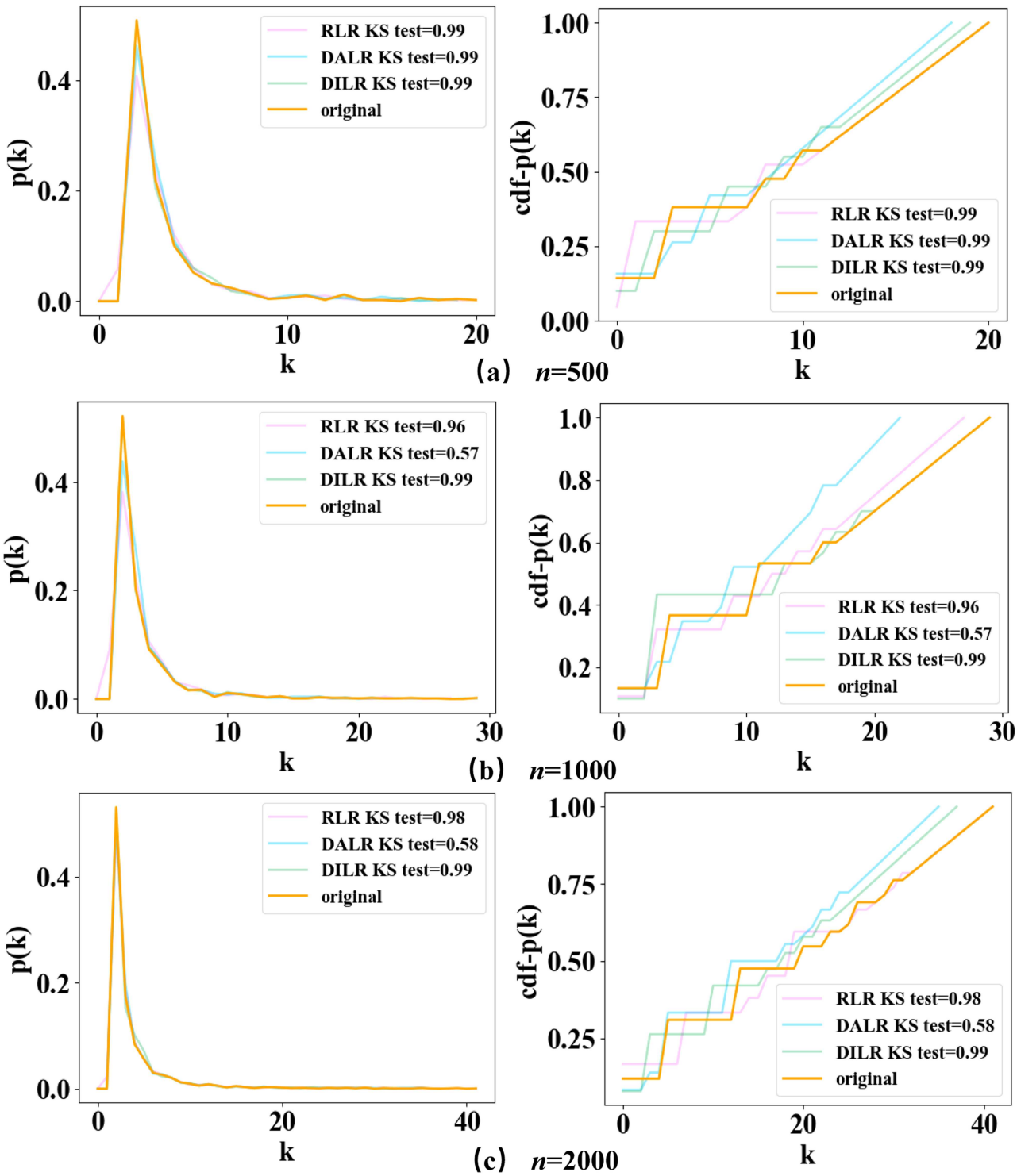

FIG. 7. The degree distributions and cdf degree distributions of the original network and adversarial networks with different sizes: (a) n=500, (b) n=1000, and (c) n=2000.

TABLE V. The metrics of concealment (ΔL, ΔC, and ΔD) when successfully attack on the BA model networks of different sizes, for different attack strategies. The best results are marked in bold for each category.

Metrics	Network size	Attack strategy	Strong→weak (%)	Strong→weakest (%)	Strong→super-weak (%)	Strong→non-scale-free (%)	Overall (%)
ΔL	$n=500$	RLR	**2.28**	**2.37**	**2.32**	**1.33**	**2.25**
		DALR	10.03	9.21	9.86	8.39	9.96
		DILR	3.31	6.58	3.81	4.10	3.67
	$n=1000$	RLR	**2.41**	**2.36**	**2.34**	**1.17**	**2.09**
		DALR	13.49	17.40	13.04	12.92	13.08
		DILR	5.72	11.27	4.64	3.23	5.07
	$n=2000$	RLR	**2.10**	**2.02**	**2.06**	**0.81**	**2.07**
		DALR	16.23	…	15.86	15.10	16.08
		DILR	9.75	16.29	5.39	3.50	7.74
ΔC	$n=500$	RLR	31.83	**29.30**	31.89	**17.64**	32.22
		DALR	60.28	57.41	61.47	52.45	60.90
		DILR	**20.82**	38.60	**23.50**	26.80	**23.91**
	$n=1000$	RLR	31.74	**32.37**	31.54	**13.35**	30.11
		DALR	68.18	87.09	68.15	64.53	67.75
		DILR	**28.96**	53.53	**24.72**	15.75	**26.62**
	$n=2000$	RLR	**28.62**	**22.41**	29.79	**9.61**	**31.56**
		DALR	71.69	…	71.76	67.33	72.85
		DILR	42.30	64.47	**23.34**	10.02	35.24
ΔD	$n=500$	RLR	**0.00**	**0.08**	**0.00**	**0.11**	**0.05**
		DALR	**0.00**	0.95	0.29	0.59	0.46
		DILR	0.02	0.40	0.06	0.26	0.06
	$n=1000$	RLR	**0.00**	**0.16**	**0.01**	0.31	0.11
		DALR	0.01	0.17	0.03	0.37	0.13
		DILR	**0.00**	0.19	**0.01**	**0.04**	**0.04**
	$n=2000$	RLR	**0.00**	1.51	0.04	**0.10**	0.41
		DALR	0.03	…	**0.02**	0.13	**0.03**
		DILR	0.03	**0.25**	0.05	0.50	0.17

All the three attack strategies introduce very small ΔD, i.e., lower than 1% for BA model networks and 10% for UCM model networks. Note that here, ΔC is relatively large for all the three attack strategies because BA scale-free networks do not have many triangular motifs, thus have very small average clustering coefficients. Consequently, a very small perturbation on a triangular structure will lead to a huge change of ΔC according to Eq. (8). To statistically compare the original networks and the adversarial networks generated by each attack strategy, the violin plots are shown for the three structural properties, i.e., L, C, and D, of the networks, both before and after an attack, as shown in Fig. 6. It is found that the shortest path-length increases and the clustering coefficient decreases after the attack, while the diagonal distance remains almost the same. This is reasonable since the attack focuses on destroying the *scale-free* property, which will weaken the dominant role of hub nodes and further increase the shortest path-length. On the other hand, the global random rewiring operations in the three strategies may also destruct triangles in these networks, leading to smaller clustering coefficients. In general, DILR has comparable concealment as RLR, both of which introduce relatively small changes of L, C, and D, while DALR causes dramatic changes of the network structures, thus could be relatively easy to detect. Besides that, the KS test is used to distinguish the degree distribution difference between the original one and the adversarial one because the BC classification method is closely related to the degree distribution. The results are shown in Fig. 7, and the KS test results are close to 1 for RLR and DILR, which means that both of these methods introduce a negligible change to the degree distribution. Although the degree distribution of the adversarial network attacked by the DALR method is different from the original degree distribution, there is no statistically significant difference.

Note that we also test the DILR adversarial attack method on real-world networks and get similar results. It is hard to get a strong or the strongest scale-free real-world network according to the BC classification; therefore, we choose three weak real-world networks obtained from Github of Adbroido[53] and where Broido

TABLE VI. The metrics of concealment (ΔL, ΔC, and ΔD) when successfully attack on the UCM model networks of different sizes, for different attack strategies. The best results are marked in bold for each category.

Metrics	Network size	Attack strategy	Strong→weak (%)	Strong→weakest (%)	Strong→super-weak (%)	Strong→non-scale-free (%)	Overall (%)
ΔL	$n=500$	RLR	**0.07**	**1.46**	**0.36**	**0.08**	**0.25**
		DALR	2.12	…	5.08	1.05	2.67
		DILR	0.93	…	1.81	1.13	1.24
	$n=1000$	RLR	**0.27**	4.39	**0.67**	**0.14**	**0.64**
		DALR	3.64	…	6.53	0.40	3.56
		DILR	1.28	**0.67**	1.47	0.82	1.30
	$n=2000$	RLR	**0.74**	…	**1.76**	**0.03**	**1.06**
		DALR	5.28	…	8.49	2.82	6.45
		DILR	2.33	…	2.84	1.34	2.36
ΔC	$n=500$	RLR	**5.46**	**13.92**	11.91	**2.88**	**5.55**
		DALR	13.44	…	35.31	4.96	12.57
		DILR	6.90	…	**3.92**	8.46	7.54
	$n=1000$	RLR	10.59	33.90	24.72	**4.83**	12.67
		DALR	24.76	…	43.22	9.21	30.45
		DILR	**8.49**	**12.92**	**12.53**	6.87	**9.87**
	$n=2000$	RLR	20.18	…	28.41	**7.82**	18.45
		DALR	35.21	…	49.14	22.71	30.91
		DILR	**16.46**	…	**19.69**	11.05	**14.32**
ΔD	$n=500$	RLR	**6.39**	**7.05**	**6.35**	**7.82**	**6.90**
		DALR	7.69	…	8.37	7.83	7.96
		DILR	8.01	…	8.57	8.08	8.22
	$n=1000$	RLR	**6.71**	13.00	**4.34**	7.80	**5.97**
		DALR	7.77	…	5.19	**7.38**	6.94
		DILR	8.12	**4.72**	6.29	8.29	7.14
	$n=2000$	RLR	**3.04**	…	**0.09**	6.28	**4.14**
		DALR	5.07	…	2.15	**5.55**	4.98
		DILR	6.72	…	5.42	6.66	6.27

obtains the real-world network[54] to attack. The results show that it is easier to be in the super-weak category than in the weakest category. Moreover, the concealment metrics are slightly changed, which means that it is hard to detect. The KS test is close to 1, indicating that we accept that the original degree distribution and the adversarial degree distribution come from the same distribution statistically.

V. CONCLUSION

This paper has discussed the robustness of the scale-free network classification method proposed by Broido and Clauset,[15] referred to as BC classification herein. In so doing, three attack strategies, RLR, DALR, and DILR, are proposed and tested. The attack experiments on strong scale-free networks generated by the BA model and the UCM model show that the BC classification method is vulnerable to adversarial attacks; e.g., only 6% links for BA model networks and less than that for UCM model networks need to be rewired to successfully attack a strong scale-free network such that it becomes the weak, the weakest, the super-weak, or even the non-scale-free network.

In addition, the BC classification result is not as good as described:[15] The cost of transforming a strong network into the weakest category is even higher than the cost of transforming it into the non-scale-free category. Moreover, the concealment metrics are changed little, although some purposefully designed noises are added, which indicates that there is no layered relationship between these categories.

This paper has examined four indicators in the BC classification method: p, n_{tail}, R, and α. Among these indicators, the values of p and α can be easily changed by slightly disturbing the network structure, while n_{tail} and R show relatively strong robustness. This results in unbalanced distributions of the adversarial networks in different categories. For instance, since the requirement of the weakest category is $n_{tail} > 50$, it is extremely difficult to attack a strong scale-free network to change it to be in the weakest category, especially when the network is relatively large. We demonstrate that it should be very careful when using p-value in the classification

method since it is sensitive to noise. Therefore, one should consider the robustness for each indicator when trying to propose a new classification method.

This study may provide a different perspective on the arguable definition of scale-free networks. We test the robustness of the BC classification by an adversarial attack method. Moreover, beyond the scale-free feature, in complex networks, there are also many other classifications derived from real-world data. Therefore, a suggestion is to adopt similar methods to test their robustness against various adversarial attacks.

ACKNOWLEDGMENTS

The authors would like to thank all the members in the IVSN Research Group, Zhejiang University of Technology, for their valuable discussions about the ideas and technical details presented in this paper. This work was partially supported by the National Natural Science Foundation of China (NNSFC) under Grant No. 61973273, by the Zhejiang Provincial Natural Science Foundation of China under Grant No. LR19F030001, and by the Hong Kong Research Grants Council under the GRF grant (No. CityU11200317).

DATA AVAILABILITY

The data that support the findings of this study are available within the article.

REFERENCES

[1]H. Ebel, L.-I. Mielsch, and S. Bornholdt, "Scale-free topology of e-mail networks," Phys. Rev. E **66**, 035103 (2002).
[2]R. Albert, "Scale-free networks in cell biology," J. Cell Sci. **118**, 4947–4957 (2005).
[3]R. Albert, H. Jeong, and A.-L. Barabási, "Internet: Diameter of the world-wide web," Nature **401**, 130 (1999).
[4]Q. Xuan, J. Wang, M. Zhao, J. Yuan, C. Fu, Z. Ruan, and G. Chen, "Subgraph networks with application to structural feature space expansion," IEEE Trans. Knowl. Data Eng. (2019).
[5]A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," Science **286**, 509–512 (1999).
[6]A.-L. Barabási, R. Albert, and H. Jeong, "Mean-field theory for scale-free random networks," Physica A **272**, 173–187 (1999).
[7]R. Molontay and M. Nagy, "Twenty years of network science: A bibliographic and co-authorship network analysis," arXiv2001.09006 (2020).
[8]P. L. Krapivsky, S. Redner, and F. Leyvraz, "Connectivity of growing random networks," Phys. Rev. Lett. **85**, 4629 (2000).
[9]A. Barabási, see https://www.barabasilab.com/post/love-is-all-you-need for "Love Is All You Need: Clauset's Fruitless Search for Scale-Free Networks," blog post (2018).
[10]R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," Phys. Rev. Lett. **86**, 3200 (2001).
[11]X. F. Wang and G. Chen, "Pinning control of scale-free dynamical networks," Physica A **310**, 521–531 (2002).
[12]Q. Xuan, Z.-Y. Zhang, C. Fu, H.-X. Hu, and V. Filkov, "Social synchrony on complex networks," IEEE Trans. Cybern. **48**, 1420–1431 (2017).
[13]S. N. Dorogovtsev and J. F. Mendes, "Evolution of networks," Adv. Phys. **51**, 1079–1187 (2002).
[14]W. Willinger, D. Alderson, and J. C. Doyle, "Mathematics and the internet: A source of enormous confusion and great potential," Not. Am. Math. Soc. **56**, 586–599 (2009).
[15]A. D. Broido and A. Clauset, "Scale-free networks are rare," Nat. Commun. **10**, 1017 (2019).
[16]E. Klarreich, "Scant evidence of power laws found in real-world networks," Quanta Mag. (15 February 2018).
[17]I. Voitalov, P. van der Hoorn, R. van der Hofstad, and D. Krioukov, "Scale-free networks well done," arXiv:1811.02071 (2018).
[18]Q. Xuan, B. Fang, Y. Liu, J. Wang, J. Zhang, Y. Zheng, and G. Bao, "Automatic pearl classification machine based on a multistream convolutional neural network," IEEE Trans. Ind. Electron. **65**, 6538–6547 (2017).
[19]Q. Xuan, Z. Chen, Y. Liu, H. Huang, G. Bao, and D. Zhang, "Multiview generative adversarial network and its application in pearl classification," IEEE Trans. Ind. Electron. **66**, 8244–8252 (2018).
[20]N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* (IEEE, 2016), pp. 372–387.
[21]J. Su, D. V. Vargas, and K. Sakurai, "One pixel attack for fooling deep neural networks," IEEE Trans. Evol. Comput. **23**, 828–841 (2019).
[22]S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "Deepfool: A simple and accurate method to fool deep neural networks," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (IEEE, 2016), pp. 2574–2582.
[23]C. Xie, J. Wang, Z. Zhang, Y. Zhou, L. Xie, and A. Yuille, "Adversarial examples for semantic segmentation and object detection," in *Proceedings of the IEEE International Conference on Computer Vision* (IEEE, 2017) pp. 1369–1378.
[24]I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," arXiv:1412.6572 (2014).
[25]A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," arXiv:1607.02533 (2016).
[26]S.-M. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, "Universal adversarial perturbations," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (IEEE, 2017) pp. 1765–1773.
[27]H. Dai, H. Li, T. Tian, X. Huang, L. Wang, J. Zhu, and L. Song, "Adversarial attack on graph structured data," arXiv:1806.02371 (2018).
[28]C. Fu, M. Zhao, L. Fan, X. Chen, J. Chen, Z. Wu, Y. Xia, and Q. Xuan, "Link weight prediction using supervised learning methods and its application to Yelp layered network," IEEE. Trans. Knowl. Data Eng. **30**, 1507–1518 (2018).
[29]J. Chen, J. Zhang, X. Xu, C. Fu, D. Zhang, Q. Zhang, and Q. Xuan, "E-LSTM-D: A deep learning framework for dynamic network link prediction," IEEE Trans. Syst. Man Cybern. Syst. (2019).
[30]X. Wang, J. Eaton, C.-J. Hsieh, and F. Wu, "Attack graph convolutional networks by adding fake nodes," arXiv:1810.10751 (2018).
[31]J. Chen, L. Chen, Y. Chen, M. Zhao, S. Yu, Q. Xuan, and X. Yang, "Ga-based q-attack on community detection," IEEE Trans. Comput. Soc. Syst. **6**, 491–503 (2019).
[32]S. Yu, M. Zhao, C. Fu, J. Zheng, H. Huang, X. Shu, Q. Xuan, and G. Chen, "Target defense against link-prediction-based attacks via evolutionary perturbations," IEEE Trans. Knowl. Data Eng. (2019).
[33]D. Zügner, A. Akbarnejad, and S. Günnemann, "Adversarial attacks on neural networks for graph data," in *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining* (ACM, 2018), pp. 2847–2856.
[34]S. Evans, P. Mills, and J. Dawson, "The end of the p value?," Br. Heart J. **60**, 177 (1988).
[35]V. Amrhein, S. Greenland, and B. McShane, "Scientists rise up against statistical significance," Nature **567**, 305–307 (2019).
[36]T. Gross, C. J. D. D'Lima, and B. Blasius, "Epidemic dynamics on an adaptive network," Phys. Rev. Lett. **96**, 208701 (2006).
[37]E. Ferrara, O. Varol, C. Davis, F. Menczer, and A. Flammini, "The rise of social bots," Commun. ACM **59**, 96–104 (2016).
[38]S. Kumar, R. West, and J. Leskovec, "Disinformation on the web: Impact, characteristics, and detection of Wikipedia hoaxes," in *Proceedings of the 25th International Conference on World Wide Web* (ACM, 2016), pp. 591–602.
[39]M. Gerlach and E. G. Altmann, "Testing statistical laws in complex systems," Phys. Rev. Lett. **122**, 168301 (2019).
[40]R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," Nature **406**, 378 (2000).

[41] R. Pastor-Satorras, A. Vespignani *et al.*, "Epidemics and immunization in scale-free networks," in *Handbook of Graphs and Networks* (Wiley-VCH, Berlin, 2003).
[42] Z. Ruan, M. Tang, and Z. Liu, "Epidemic spreading with information-driven vaccination," Phys. Rev. E **86**, 036117 (2012).
[43] M. Wolfson, A. Budovsky, R. Tacutu, and V. Fraifeld, "The signaling hubs at the crossroad of longevity and age-related disease networks," Int. J. Biochem. Cell Biol. **41**, 516–520 (2009).
[44] G. Bianconi and A.-L. Barabási, "Bose-Einstein condensation in complex networks," Phys. Rev. Lett. **86**, 5632 (2001).
[45] X. Li and G. Chen, "A local-world evolving network model," Physica A **328**, 287–296 (2003).
[46] Q. Xuan, Y. Li, and T.-J. Wu, "Growth model for complex networks with hierarchical and modular structures," Phys. Rev. E **73**, 036105 (2006).
[47] Q. Xuan, Y. Li, and T.-J. Wu, "A local-world network model based on inter-node correlation degree," Physica A **378**, 561–572 (2007).
[48] Q. Sen and G.-Z. Dai, "A new local-world evolving network model," Chin. Phys. B **18**, 383 (2009).
[49] M. Catanzaro, M. Boguná, and R. Pastor-Satorras, "Generation of uncorrelated random scale-free networks," Phys. Rev. E **71**, 027103 (2005).
[50] J. Ugander, B. Karrer, L. Backstrom, and C. Marlow, "The anatomy of the Facebook social graph," arXiv:1111.4503 (2011).
[51] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," Nature **393**, 440 (1998).
[52] D. Tsiotas, "Detecting different topologies immanent in scale-free networks with the same degree distribution," Proc. Natl. Acad. Sci. U.S.A. **116**, 6701–6706 (2019).
[53] See https://github.com/adbroido/SFAnalysis for "Scale-Free Network Analysis."
[54] See https://icon.colorado.edu for "The Colorado Index of Complex Networks (ICON)."