# Robustness of preferential-attachment graphs

**Journal Article**

**Author(s):**
Hasheminezhad, Rouzbeh; Brandes, Ulrik

**Publication date:**
2023-06-13

**Permanent link:**
https://doi.org/10.3929/ethz-b-000618134

**Originally published in:**
Applied Network Science 8(1), https://doi.org/10.1007/s41109-023-00556-5

Hasheminezhad and Brandes
*Applied Network Science* (2023) 8:32
https://doi.org/10.1007/s41109-023-00556-5

Applied Network Science

RESEARCH Open Access

# Robustness of preferential-attachment graphs

Rouzbeh Hasheminezhad[1]* and Ulrik Brandes[1]

A preliminary version of this paper has appeared in Hasheminezhad and Brandes (2023).

*Correspondence: shashemi@ethz.ch

[1] Social Networks Lab, ETH Zürich, Zurich, Switzerland

**Abstract**

The widely used characterization of scale-free networks as "robust-yet-fragile" originates primarily from experiments on instances generated by preferential attachment. According to this characterization, scale-free networks are more robust against random failures but more fragile against targeted attacks when compared to random networks of the same size. Here, we consider a more appropriate baseline by requiring that the random networks match not only the size but also the inherent minimum degree of preferential-attachment networks they are compared with. Under this more equitable condition, we can (1) prove that random networks are almost surely robust against any vertex removal strategy and (2) show through extensive experiments that scale-free networks generated by preferential attachment are not particularly robust against random failures. Finally, we (3) add experiments demonstrating that preferentially attaching to well-connected vertices does not enhance robustness at all.

**Keywords:** Robustness, Scale-free networks, Preferential attachment

## Introduction

Although preferential attachment models can generate only a vanishing fraction of all scale-free networks (Petersen et al. 2016), many claims about the class of scale-free networks arise from experiments on preferential-attachment instances. One such claim, originating from Albert et al. (2000), is that scale-free networks have a "robust-yet-fragile" nature, i.e., compared to random networks of the same size, they are more robust against random failures, where vertices are removed uniformly at random, but more fragile against targeted attacks, where vertices with the highest initial degree are removed first (Doyle et al. 2005).

The common models for preferential attachment, including the one used in the experiments of Albert et al. (2000), yield instances with a constant average degree and a minimum degree of half that value. Because of their constant average degree, however, random networks of the same size are highly likely to contain isolated vertices (Erdős and Rényi 1959). As a first contribution, we prove that the robustness and connectivity of such random networks change significantly if they are required to have a minimum degree of at least $k$ for any constant $k \geq 3$. With this in mind, it seems more appropriate and natural to compare the robustness of preferential-attachment instances with random networks of the same size *and the same minimum degree*. To the best of our knowledge, this has not yet been done. We fill this gap with our second contribution through an extensive suite of experiments. Our experiments show, in the affirmative, that scale-free instances generated by preferential attachment are consistently more fragile than size-matching random networks whose minimum degree is at least as large. To put it more bluntly: We find that in an equitable setting, the networks generated by preferential attachment do not exhibit a "robust-yet-fragile" nature.

As our last contribution, we carry out experiments, which demonstrate that a preference for attachment to well-connected others does not enhance robustness in any way. Our contributions can be formally summarized as follows:

1 For any constant $k \geq 3$, almost all graphs with a constant average degree and a minimum degree of at least $k$ are connected and provably robust.
2 Scale-free networks generated by preferential attachment are more fragile than size-matching random graphs whose minimum degree is at least as large.
3 Preferential attachment leads to lower robustness than random attachment.

## Preliminaries

We use $\mathbb{N}$ to denote the set of positive integers. We use $\lfloor x \rceil$ to denote the integer closest to $x$, breaking the ties in favor of higher values. More precisely, $\lfloor x \rceil = \lceil x \rceil$ if $x - \lfloor x \rfloor \geq 0.5$ and $\lfloor x \rceil = \lfloor x \rfloor$ otherwise. When we say that a statement holds for large enough $n \in \mathbb{N}$, there exists a constant $n_0 \in \mathbb{N}$ such that the statement holds for all $n$ that are larger than $n_0$. We say that a sequence of events $\mathcal{A}_n$ holds almost surely if $\lim_{n\to\infty} \Pr[\mathcal{A}_n] = 1$.

### Graphs and degree sequences

In this paper, we consider only simple undirected graphs and use the terms graph and network interchangeably. A graph $G = (V, E)$ consists of a set of vertices $V$ and a set of edges $E \subseteq \binom{V}{2}$. If $\{u, w\} \in E$, then $u$ and $w$ are said to be adjacent. A graph is called complete if each vertex is adjacent to all other vertices. The degree, $\deg_G(v)$, of a vertex $v$ is the number of vertices in $G$ adjacent to $v$. If $v_1, \cdots, v_n$ is an ordering of $V$ where $\deg(v_1) \geq \cdots \geq \deg(v_n)$, then $D(G) = \big(\deg(v_1), \ldots, \deg(v_n)\big)$ is the degree sequence of $G$. An integer sequence $D$ is called graphical if there is a simple undirected graph $G$ with $D = D(G)$. We use $\Delta(G)$ and $\delta(G)$ to denote, respectively, the maximum and minimum vertex degree in $G$. The graph $G$ is called $k$-regular if $\delta(G) = \Delta(G) = k$.

The subgraph of a graph $G = (V, E)$ induced by $V' \subseteq V$ is $G[V'] = (V', E')$, where $E' = \big\{\{u, w\} \in E | u, w \in V'\big\}$. Given a positive integer $k$, the $k$-core of a graph $G$ is the inclusion-maximal induced subgraph, where all vertex degrees are at least $k$. The $k$-core of a graph is unique and can be determined efficiently (Batagelj and Zaveršnik 2011).

The reachability relation is defined as the reflexive and transitive closure of the adjacency relation. The connected components of a graph are its subgraphs induced by the equivalence classes of the reachability relation. A graph is called connected if it consists of a single connected component. The largest connected component, or LCC for short, is the one with the largest number of vertices.

### Network robustness

The extent of invariance of a network structural property when elements of the network are removed is referred to as the robustness of that network (Klau and Weiskircher 2005). We focus only on the removal of vertices and consider the number of vertices in the largest connected component as the structural property of interest.

Given a connected graph $G = (V, E)$ and the sequence of vertices $B = (b_1, b_2, \ldots, b_T)$ in order of their removal, we can quantify the robustness of $G$ by

$$R_G(B) = \frac{1}{T} \sum_{t=1}^{T} \frac{|\mathrm{LCC}(G[V \backslash \{b_1, \ldots, b_t\}])|}{|\mathrm{LCC}(G)|}.$$

This robustness score originally proposed in Hasheminezhad and Brandes (2022) is a generalization of the score used in Schneider et al. (2011), where in the latter score, $B$ is a permutation of $V$. Note that the above score captures the relative size of the largest connected component and the rate at which it shrinks when the vertices are removed. The most commonly considered vertex removal strategies in the literature are random failures and targeted attacks. In random failures, the vertices are removed uniformly at random. In targeted attacks, the vertices with the highest initial degree are removed first. If the vertex removal strategy is clear from the context, and we accept random variation in vertex selection due to the tie-breaking rules, we can parameterize the robustness score by the fraction $\beta$ of removed vertices rather than by the precise sequence.

Note that the complete graph has the highest robustness among all $n$-vertex connected graphs, as it remains connected through any vertex removal process. For such a graph, $R_G(B)$ is given by $1 - \frac{|B|+1}{2n}$, which simplifies to $1 - \beta/2 + o(1)$ if the fraction of removed vertices is $\beta$, i.e., when $|B| = \beta n$. It follows that $R_G(\beta)$ is upper-bounded by $1 - \beta/2 + o(1)$ for any connected graph $G$ and any vertex removal strategy (Hasheminezhad et al. 2020).

The (vertex) isoperimetric number $h(G)$ and the conductance $\Phi(G)$ are invariants closely related to the robustness of a graph $G = (V, E)$. The former is defined as $h(G) = \min_{\emptyset \neq S \subset V, |S| \leq \frac{|V|}{2}} \left\{ \frac{|\partial S|}{|S|} \right\}$ where $\partial S$ is the subset of vertices in $V \backslash S$ that are adjacent to at least one vertex in $S$. Similarly, $\Phi(G)$ is defined as $\Phi(G) = \min_{\emptyset \neq S \subset V, |S| \leq \frac{|V|}{2}} \left\{ \frac{|E(S, V \backslash S)|}{\mathrm{vol(S)}} \right\}$ where $\mathrm{vol(S)} = \sum_{\mathrm{v} \in \mathrm{S}} \deg_G(\mathrm{v})$ and $E(S, V \backslash S)$ is the subset of edges in $E$ with one endpoint in $S$ and the other in $V \backslash S$. It is well known that $h(G) \geq \frac{\delta(G)}{\Delta(G)} \Phi(G)$ (see FACT A.1. in Giakkoupis and Sauerwald 2012 for a brief proof of this).

### Network models

The set of simple graphs with $n$ vertices and $m$ edges is denoted by $G(n, m)$, and $G(n, m, k)$ is the subset of graphs in $G(n, m)$ that have a minimum degree of at least $k$. The models $\mathsf{G}(n, m)$ and $\mathsf{G}(n, m, k)$ consist of the uniform distribution on $G(n, m)$ and $G(n, m, k)$, respectively.

Scale-free networks are those networks in which the fraction of vertices with degree $k$ is roughly proportional to $k^{-\gamma}$ for some $\gamma > 1$. Since its popularization by Barabási and Albert (1999), preferential attachment has been the most widely used mechanism for generating scale-free networks. Although there are several instantiations of the same general idea, here we adhere to the approach used in the original robustness experiments of Albert et al. (2000). This generative preferential-attachment model $\mathsf{PA}(n, k)$ starts from a complete graph with $2k + 1$ vertices and successively adds $n - (2k + 1)$ vertices. Each newly added vertex is made adjacent to $k$ distinct vertices, drawn without replacement from the pool of existing vertices and with a probability that is proportional to their current degree. All graphs generated in this way are connected, have a minimum degree of $k$, $m = kn$ edges (an average degree of $2k$), and are thus elements of $G(n, nk, k)$.

To assess their relative robustness, preferential attachment graphs are often pitted against random size-matching graphs drawn from $\mathsf{G}(n, m)$. If the number of edges is bounded linearly and away from one, i.e., $m = kn$ for some constant $k > 1$, random graphs are unlikely to be connected, but they almost surely have a unique giant component (Erdős and Rényi 1959; Molloy and Reed 1998). This is also acknowledged in the robustness experiments of Albert et al. (2000), where rejection sampling is used to find a graph with a large enough largest connected component. So, while size and connectivity are largely kept constant in experiments on network robustness, the minimum-degree property of preferential-attachment graphs has not been considered. In "Theory" section, we show that this can be expected to have a major influence on what can reasonably be considered robust.

## Network generation

We construct $\mathsf{PA}(n, k)$ and $\mathsf{G}(n, m)$ graphs using linear-time algorithms (Batagelj and Brandes 2005). In this section, we provide the details of the algorithm we use to sample from $\mathsf{G}(n, m, k)$. To this end, we first introduce a basic approach in "The straightforward approach" section and explain why this method was not utilized. Subsequently, we present a slightly more sophisticated method in "The efficient approach" section, which we use to efficiently draw samples from $\mathsf{G}(n, m, k)$.

### *The straightforward approach*

One way to generate a graph from $\mathsf{G}(n, m)$ is to use a variant of the Bollobás configuration model (Bollobás 1980), also known as the random sequence model. This model generates a sequence $(x_1, x_2, \ldots, x_{2m})$ in which the elements are sampled uniformly at random from the set of vertices $V = \{v_1, \ldots, v_n\}$ and the edges consist of $E = \{\{x_i, x_{i+1}\} | i \in \{1, 2, \ldots, m\}\}$. Conditioned on the resulting graph being simple (without duplicate edges and self-loops), the generated graphs are sampled exactly uniformly from $G(n, m)$. This procedure can also be viewed as a balls and bins process, explained below.

1 Let $e_1, \ldots, e_m$ represent the edges to be added. Let $e_{t,1}, e_{t,2}$ represent the half-edges (also known as stubs) corresponding to $e_t$, where $t \in \{1, \ldots, m\}$.
2 Assign half-edges to the $n$ vertices $v_1$, ..., $v_n$ uniformly at random.
3 If $e_{t,1}$ is assigned to $v_i$ and $e_{t,2}$ to $v_j$, then add an edge between $v_i$ and $v_j$.
4 If the resulting graph is simple, output it; otherwise, restart from step one.

To modify this procedure for sampling from $\mathsf{G}(n, m, k)$, it suffices to modify the second step above by randomly assigning half-edges to the $n$ vertices, with the additional condition that each vertex has at least $k$ half-edges assigned. If $2m = cn$ and $c \geq k \geq 1$ for some constants $c$ and $k$, the probability that the resulting graph is simple in the last step is $\Omega(1)$ (Bollobás et al. 2000). Therefore, this approach requires $O(n)$ time in expectation to sample from $\mathsf{G}(n, m, k)$. Although this approach is straightforward and theoretically efficient, based on our implementation, it is quite inefficient in practice. This is likely due to the large constants hidden by the asymptotic notation.

### *The efficient approach*

Here, we present a detailed exposition of an algorithm that leverages a theoretical result from Janson and Luczak (2008) to efficiently sample from $\mathsf{G}(n, nk, k)$, where $k \geq 3$ is some constant. Consider a graph $G$, which is the $k$-core of a larger graph drawn from $\mathsf{G}(\tilde{n}, \tilde{m})$. The $k$-core may be either empty or have a distribution $\mathsf{G}(\upsilon, \mu, k)$ with $\upsilon$ and $\mu$ denoting the (random) number of vertices and edges in the $k$-core, respectively (Anastos and Frieze 2020). In case we condition on $\upsilon = n$ and $\mu = m$, the distribution of $G$ is equivalent to $\mathsf{G}(n, m, k)$. In Algorithm 1, we exploit the last observation to efficiently sample from $\mathsf{G}(n, nk, k)$ by using rejection sampling and selecting appropriate values of $\tilde{n}$ and $\tilde{m}$ based on Theorem 1 (Theorem 1.1 of Janson and Luczak (2008)) such that the event $\upsilon = n$ and $\mu = nk$ occurs almost surely. To state Theorem 1, we define $\psi_k(x) := 1 - e^{-x} \sum_{i=1}^{k-1} \frac{x^i}{i!}$ and $c_k := \min_{x>0} \phi_k(x)$, where $\phi_k(x) := \frac{x}{\psi_{k-1}(x)}$. These functions are essential in characterizing the threshold for the emergence of $k$-cores in random graphs.

**Theorem 1** (Janson and Luczak 2008) *Let $G$ be a graph drawn from $\mathsf{G}(n, m)$ where $2\,m = cn$ for some constant $c$. Furthermore, let $k \geq 3$ be a constant and assume that $n$ is large enough. If $c < c_k$, then the $k$-core of $G$ is almost surely empty. On the other hand, if $c > c_k$, then the $k$-core of $G$ almost surely contains $\psi_k(x^*)n$ vertices and $\frac{1}{2}x^*\psi_{k-1}(x^*)n$ edges, where $x^*$ is the largest among the two unique solutions of $\phi_k(x) = c$.*

**Algorithm 1:** Efficient sampling from $\mathsf{G}(n, m, k)$

```
Input: Positive integers $n, m, k$ where $m = kn$ and $k \geq 3$.
Output: The graph $G$ sampled uniformly from $G(n, m, k)$.
1 $x \leftarrow \hat{x}$ s.t. $f(\hat{x}) = 0$ where $f(x) := \frac{\hat{x}\psi_{k-1}(\hat{x})}{\psi_k(x)} - 2k$        // To ensure $\frac{\eta}{\upsilon}$ is $k$
2 $\tilde{n} \leftarrow \lfloor \frac{n}{\psi_k(x)} \rceil$        // To ensure $\upsilon$ is concentrated sharply around $n$
3 $\tilde{m} \leftarrow \lfloor \frac{\phi_k(x)\tilde{n}}{2} \rceil$        // Incorporating the constraint that $\tilde{m} = \frac{1}{2}c\tilde{n}$ where $c = \phi_k(x)$
4 do
5     $\tilde{G} \sim \mathsf{G}(\tilde{n}, \tilde{m})$        // Uniformly sample a graph $\tilde{G}$ with $\tilde{n}$ vertices and $\tilde{m}$ edges
6     $G = (V, E) \leftarrow$ k-core$(\tilde{G})$
7 while $|V| \neq n, |E| \neq m$
8 return $G$
```

Note that we use the bisection method to efficiently attain the value of $x$ on line 1 of Algorithm 1 utilizing the fact that $f(x)$, as defined in Algorithm 1, is monotonically decreasing and has a root in $(k, 2k)$, based on Lemma A1 in Bollobás et al. (2000).

In this section, we proposed Algorithm 1 to sample uniformly from $G(n, nk, k)$ based on Theorem 1 for any constant $k \geq 3$. However, the algorithm lacks explicit verification of certain conditions of Theorem 1, for instance, whether $\phi_k(x) = c > c_k$ for $k \geq 3$ when $x$ is selected as in Algorithm 1. Therefore, we could not establish probabilistic bounds on the algorithm's running time or theoretically guarantee that the algorithm terminates at all. Nevertheless, for any constant $k \geq 3$, the algorithm samples exactly uniformly from $G(n, nk, k)$ conditioned on successful termination, as implied by the argument presented at the beginning of the section. Our empirical evaluations of the algorithm demonstrate that its termination time is reasonable for the range of $k$ studied in our experiments.

## Theory

Under the condition that the minimum degree is at least $k$ for a constant $k \geq 3$, we show in Theorem 2 that almost all graphs with a constant average degree are not only connected but also provably robust against any vertex removal strategy.

In the following paragraph, we briefly outline the key intermediary results and how they are used to lead up to Theorem 2.

By using the results of Benjamini et al. (2014), we first demonstrate in Lemma 1 that a random graph conditioned on having a degree sequence of size $n$, where all elements are between 3 and $n^{0.02}$, has a conductance that is lower-bounded by a constant $\alpha > 0$. Then we use Lemma 1 to show in Lemma 2 that almost all graphs on $n$ vertices with a constant average degree and a minimum degree of at least $k \geq 3$ have $\Omega(1/\log n)$ vertex expansion. A corollary of Lemma 2.2 in Friedman and Krivelevich (2021), stated in this section as Lemma 3, allows us to use this vertex expansion property to establish provable robustness in Theorem 2.

**Lemma 1** *Given a graphical sequence* $D = (d_1, \ldots, d_n)$ *with* $\sum_{i=1}^{n} d_i \in O(n)$ *and* $n^{0.02} \geq d_1 \geq d_n \geq 3$, *there exists a constant* $\alpha > 0$ *such that for sufficiently large* $n$, *a random simple graph* $G$ *with degree sequence* $D$ *almost surely satisfies* $\Phi(G) \geq \alpha$.

***Proof***

*Let* $\mathcal{M}$ *be a graph with degree sequence* $D$ *generated via the random pairing model. This model assigns* $d_i$ *dots to each vertex in the set* $\{v_1, v_2, \ldots, v_n\}$*, and then pairs the dots uniformly at random. An edge is drawn between vertex* $v_i$ *and vertex* $v_j$ *for each dot corresponding to the i-th vertex paired with a dot corresponding to the j-th vertex. This can result in multiple edges between two vertices, as well as some vertices having self-loops. However, conditioned on* $\mathcal{M}$ *being simple, it is distributed exactly uniformly among all simple graphs with degree sequence* $D$.

Let $A_\alpha$ denote the event that there exists a constant $n_0 \in \mathbb{N}$ such that $\Phi(\mathcal{M}) < \alpha$ for all $n \geq n_0$, and let $\mathcal{B}$ denote the event that $\mathcal{M}$ is simple. In light of the above observation, it suffices to show $\mathsf{Pr}(\mathcal{A}_\alpha | \mathcal{B}) \in o(1)$ for some constant $\alpha > 0$. Since $\sum_{i=1}^{n} d_i \in O(n)$, we can use Lemma 5.2 in Benjamini et al. (2014) to obtain $\mathsf{Pr}(\mathcal{B}) \in \Omega(1)$. Therefore

$$\Pr(\mathcal{A}_\alpha|\mathcal{B}) = \frac{\Pr(\mathcal{A}_\alpha \cap \mathcal{B})}{\Pr(\mathcal{B})} \leq \frac{\Pr(\mathcal{A}_\alpha)}{\Pr(\mathcal{B})} \in O(\Pr(\mathcal{A}_\alpha)).$$

Under our assumptions, Lemma 5.3 in Benjamini et al. (2014) implies there is a constant $\vartheta > 0$ such that $\Pr(\mathcal{A}_\vartheta) \in o(1)$. Given this, the above inequality yields $\Pr(\mathcal{A}_\vartheta|\mathcal{B}) \in o(1)$. □

Lemma 2 states that, for a constant $k \geq 3$, almost all graphs with constant average degree and a minimum degree of at least $k$ exhibit $\Omega(1/\log n)$ vertex expansion. To prove Lemma 2, we show that such graphs almost surely satisfy the degree sequence conditions specified in Lemma 1 and have a maximum degree of $o(\log n)$. We then complete the proof by combining Lemma 1 with the inequality $h(G) \geq \frac{\delta(G)}{\Delta(G)}\Phi(G)$, which holds for any graph $G$.

**Lemma 2** *Let $G$ be a graph drawn from $\mathsf{G}(n, m, k)$, where $2m = cn$ and $c \geq k \geq 3$ for some constants $c, k$. If $n$ is large enough, then almost surely $h(G) \in \Omega(1/\log n)$.*

***Proof***

*Note that $\delta(G) \geq 3$ and $h(G) \geq \frac{\delta(G)}{\Delta(G)}\Phi(G)$. Therefore, it is sufficient to show that there is almost surely a constant $\alpha > 0$ such that if $n$ is large enough, then $\Pr\left[(\Phi(G) < \alpha) \bigcup (\Delta(G) > \log n)\right] \in o(1)$. By applying the union bound, we have*

$$\Pr\left[(\Phi(G) < \alpha) \bigcup (\Delta(G) > \log n)\right] \leq \Pr[\Phi(G) < \alpha] + \Pr[\Delta(G) > \log n].$$

Therefore, it suffices to show that there is almost surely a constant $\alpha > 0$ such that if $n$ is large enough, then $\Pr[\Phi(G) < \alpha] \in o(1)$ and $\Pr[\Delta(G) > \log n] \in o(1)$.

We first show $\Pr[\Delta(G) > \log n] \in o(1)$. To this end, part (ii) of Lemma 1 in Bollobás et al. (2000) suggests that, under the assumptions of the theorem, it is sufficient to show that the maximum occupancy of a box (or bin) is $o(\log n)$ in a model called $\mathcal{O}(n, 2m, k)$. In this model, $2m$ balls are thrown uniformly at random into $n$ bins, conditioned on each bin having at least $k$ balls. Within the proof of Lemma 1 in Bollobás et al. (2000), it is explicitly stated that: The maximum occupancy of any box in $\mathcal{O}(n, 2m, k)$ is $o(\log n)$ with the probability of the complementary event $n^{-O(\log\log n)}$. This establishes that $\Pr[\Delta(G) > \log n] \in o(1)$, as we wanted to show. Next, we prove $\Pr[\Phi(G) < \alpha] \in o(1)$.

Let $\xi_\alpha$ be the event that there exists a constant $n_0 \in \mathbb{N}$ such that $\Phi(G) < \alpha$ for all $n \geq n_0$. Consider $\mathcal{D} = \{D(G) : G \in G(n, m, k)\}$ and let $\widetilde{\mathcal{D}}$ be a subset of degree sequences in $\mathcal{D}$ where the maximum degree is at most $\log n$. We can write $\Pr[\xi_\alpha]$ as

$$\underbrace{\sum_{d \in \mathcal{D} \setminus \tilde{\mathcal{D}}} \Pr[\xi_\alpha | D(G) = d] \Pr[D(G) = d]}_{:= \mathcal{A}_\alpha} + \underbrace{\sum_{d \in \tilde{\mathcal{D}}} \Pr[\xi_\alpha | D(G) = d] \Pr[D(G) = d]}_{:= \mathcal{B}_\alpha}.$$

We prove that $\mathcal{A}_\alpha \in o(1)$ and $\mathcal{B}_\alpha \in o(1)$, for some constant $\alpha > 0$. Note that

$$\mathcal{A}_\alpha := \sum_{d\in\mathcal{D}\setminus\tilde{\mathcal{D}}} \underbrace{\Pr[\xi_\alpha|D(G)=d]}_{\leq 1} \Pr[D(G)=d] \leq \sum_{d\in\mathcal{D}\setminus\tilde{\mathcal{D}}} \Pr[D(G)=d].$$

The right-hand side of the above inequality is $\Pr[\Delta(G) > \log n]$, which we have shown is asymptotically zero, under our assumptions. Hence, $\mathcal{A}_\alpha \in o(1)$. Note that

$$\begin{aligned}\mathcal{B}_\alpha &:= \sum_{d\in\tilde{\mathcal{D}}} \Pr[\xi_\alpha|D(G)=d]\Pr[D(G)=d] \\ &\leq \max_{d\in\tilde{\mathcal{D}}} \Pr[\xi_\alpha|D(G)=d] \underbrace{\sum_{d\in\tilde{\mathcal{D}}} \Pr[D(G)=d]}_{\Pr\left[D(G)\in\tilde{\mathcal{D}}\right]\leq 1} \leq \max_{d\in\tilde{\mathcal{D}}} \Pr[\xi_\alpha|D(G)=d].\end{aligned}$$

As the assumptions of Lemma 1 are satisfied for all $d \in \tilde{\mathcal{D}}$, we can use it to show the existence of a constant $\vartheta > 0$ such that the right-hand side of the inequality above is asymptotically zero for $\alpha = \vartheta$. Therefore, we have $\Pr[\xi_\vartheta] = \mathcal{A}_\vartheta + \mathcal{B}_\vartheta \in o(1)$. □

Lemma 3 can be viewed as a direct corollary of Lemma 2.2 in Friedman and Krivelevich (2021), by observing that the notion of $(\frac{n}{2}, \nu)$-expander in Friedman and Krivelevich (2021) is equivalent to the definition of $\nu$-vertex expander given in this paper. Using Lemma 3 and the expansion properties of graphs drawn from $\mathsf{G}(n, m, k)$, as stated in Lemma 2, we can prove Theorem 2.[1]

**Lemma 3** (Friedman and Krivelevich 2021) *Let $G = (V, E)$ be a $\nu$-expander graph with $n$ vertices, where $0 < \nu \leq 1$. For any $0 < \epsilon \leq \frac{\nu^2}{16}$ and $V_0 \subseteq V$ with $|V_0| \leq \epsilon n$, there exists $U \subseteq V\setminus V_0$ such that $|U| \geq (1 - \frac{3\epsilon}{\nu})n$ and $G[U]$ is a $\frac{\nu}{2}$-expander.*

**Theorem 2** *Let $G$ be a graph drawn from $\mathsf{G}(n, m, k)$, where $2m = cn$ and $c \geq k \geq 3$ for some constants $c$, $k$. If $n$ is large enough, then almost surely, $G$ is connected and $R_G(B) = 1 - o(1)$ for any vertex sequence $B$ that satisfies $|B| \in o(n/\log^2 n)$.*

***Proof***

*By Lemma 2, $G$ is almost surely a $\nu$-expander where $\nu = \frac{\alpha}{\log n}$ for some constant $\alpha > 0$. Since $n$ is assumed to be large enough, it suffices to show that for $0 < \nu \leq 1$, the claims of the theorem hold when $G$ is a $\nu$-expander with $n$ vertices.*

For the sake of contradiction, assume $G$ is not connected; then, it must have at least two connected components. Let $A$ be the component with the smallest number of vertices. Obviously, $\partial A = \emptyset$ and $|A| \leq n/2$. However, since $G$ is a $\nu$-expander with $\nu > 0$ and

[1] A weaker version of Theorem 1 in our preliminary paper (Hasheminezhad and Brandes 2023) contained an error in the proof, which arose from the incorrect use of Lemma 5.3 from Benjamini et al. (2014). Although the lemma provides a statement on conductance, it was erroneously used directly to argue about vertex expansion, leading to the possibly incorrect conclusion that for some constant $\alpha > 0$, almost all graphs $G$ drawn from $\mathsf{G}(n, m, k)$ satisfy $h(G) \geq \alpha$, under the assumptions of the theorem. We have now rectified this issue by using a well-known inequality that makes a connection between the concepts of vertex expansion and conductance. Although our revised approach can only establish an almost sure vanishing vertex expansion, we could adapt our analysis to provide improved theoretical guarantees compared to the preliminary version of the paper.

$|A| \leq n/2$, we have $|\partial A| \geq \nu|A| > 0$, which contradicts $\partial A = \emptyset$. Given that assuming $G$ is not connected leads to a contradiction, $G$ must be connected.

It remains to show the second part of the theorem. If $|B| = 0$, we are done. So, we assume $|B| > 0$ and let $V_0$ denote the set of vertices in $B$. Since $n$ is assumed to be sufficiently large and $|B| = |V_0| \in o(n/\log^2 n)$, we can assume $|V_0| \leq \epsilon n$, where $\epsilon = \frac{\nu^2}{16}$. Given that all the requirements of Lemma 3 are met, we can apply it to conclude the existence of $U \subseteq V \setminus V_0$ such that $G[U]$ is a $\frac{1}{2}\nu$-vertex expander and $|U| \geq (1 - \frac{3\epsilon}{\nu})n$. By an argument similar to the one presented in the previous paragraph, we can conclude that $G[U]$ is connected. Therefore, the largest connected component of $G[V \setminus V_0]$ must also contain at least $(1 - \frac{3\epsilon}{\nu})n$ or equivalently $(1 - \frac{3\nu}{16})n$ vertices. Given the definition of $R_G(B)$, this concludes the proof. □

We can see from Theorem 2, that a graph drawn from $G(n, m, k)$ almost surely has asymptotically optimal robustness when the fraction of vertices removed is $o(n/\log^2 n)$ (e.g., when at most $n^{0.99}$ vertices are removed).

In studies on the robustness of networks such as Albert et al. (2000), scale-free instances with a constant average degree are compared to size-matching random networks. It is known that such random networks with a constant average degree are almost surely disconnected (Erdős and Rényi 1959; Molloy and Reed 1998). However, our results in this section suggest that such random networks become both connected and provably robust when their minimum degree is constrained. Therefore, the conclusions of Albert et al. (2000) may change significantly in a fairer setting where size-matching random networks also have a minimum degree at least as large as that of scale-free instances compared to them. This observation was one of the main motivations for our experiments in "Experiments" section.

## Experiments

The conclusions in Albert et al. (2000) primarily stemmed from experiments on synthetic scale-free networks generated by $\mathsf{PA}(n, k)$. We use the same model of synthetic networks to compare the robustness of preferential-attachment networks with size-matching random networks and random networks of the same size whose minimum degree is at least as large. To this end, we generate 100 networks using the model $\mathsf{PA}(n, k)$ with $n = 10{,}000, k = 3$, and then draw an equal number of networks from $\mathsf{G}(n, m)$ and $\mathsf{G}(n, m, k)$, respectively, where $m = nk$.[2] For each of the 300 networks, we then compute their robustness scores under random failures and targeted attacks, where the fraction of removed vertices is $\beta \in \{0.05, 0.1, 0.2\}$.

The results shown in Fig. 1 confirm that preferential-attachment networks are "robust-yet-fragile" when compared to random graphs of the same size, i.e., they are more fragile against targeted attacks but more robust against random failures. However, such networks are more vulnerable against both, targeted attacks and random

[2] When sampling random graphs from $\mathsf{G}(n, m)$, we reject instances with less than 96% of their vertices in the largest connected component and discard all vertices outside the largest connected component. Note that such steps are essential to ensure an equitable setting, where the generated random graphs are initially connected and have roughly the same size as the preferential-attachment graphs compared to them.

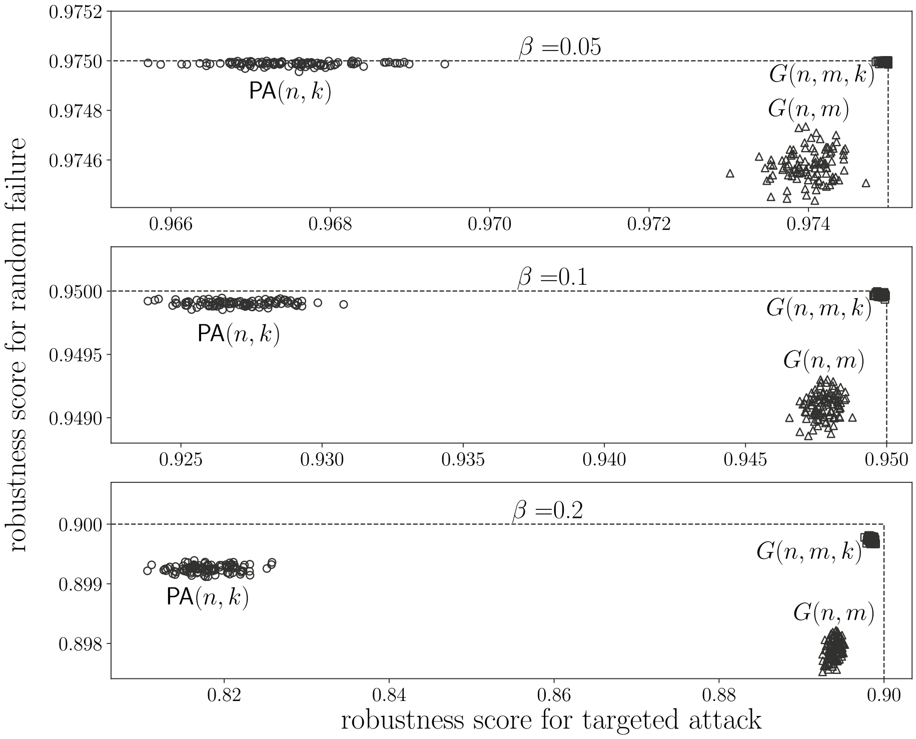

**Fig. 1** Robustness of networks generated from PA$(n,k)$ compared to networks drawn from G$(n,m)$ and G$(n,m,k)$ after 5%, 10%, and 20% of vertices were removed in targeted attacks or random failures, where $n = 10{,}000$, $m = 30{,}000$, and $k = 3$. The dashed lines represent the upper bounds for the robustness score as given in "Network robustness" section

failures, than size-matching random networks constrained to have at least the same minimum degree. We corroborate this finding in the following sections under varying conditions.

Note that the minimum degree of graphs appears to be a crucial property for their robustness. This is suggested asymptotically by Theorem 2 and is empirically evidenced, since the robustness scores of the graphs drawn from G$(n,m,k)$ are very close to the theoretical upper bounds indicated by dashed lines. This is further investigated in "Consistency of near-optimal robustness" section.

## Sensitivity to the choice of the fraction of removed vertices

In this section, we evaluate the sensitivity of our observed patterns in Fig. 1 to the choice of the proportion of removed vertices. For this purpose, we repeat the procedure to create Fig. 1, but instead of choosing moderate proportions of removed vertices $\beta \in \{0.05, 0.1, 0.2\}$, we choose relatively higher proportions by increasing each previously considered proportion by 0.2, i.e., we consider $\beta \in \{0.25, 0.3, 0.4\}$. The result is shown in Fig. 2, from which we observe that the claimed patterns based on Fig. 1 still hold in general. The main difference is that the robustness of the random networks drawn from G$(n,m,k)$ becomes less optimal when the proportion of removed vertices increases noticeably.

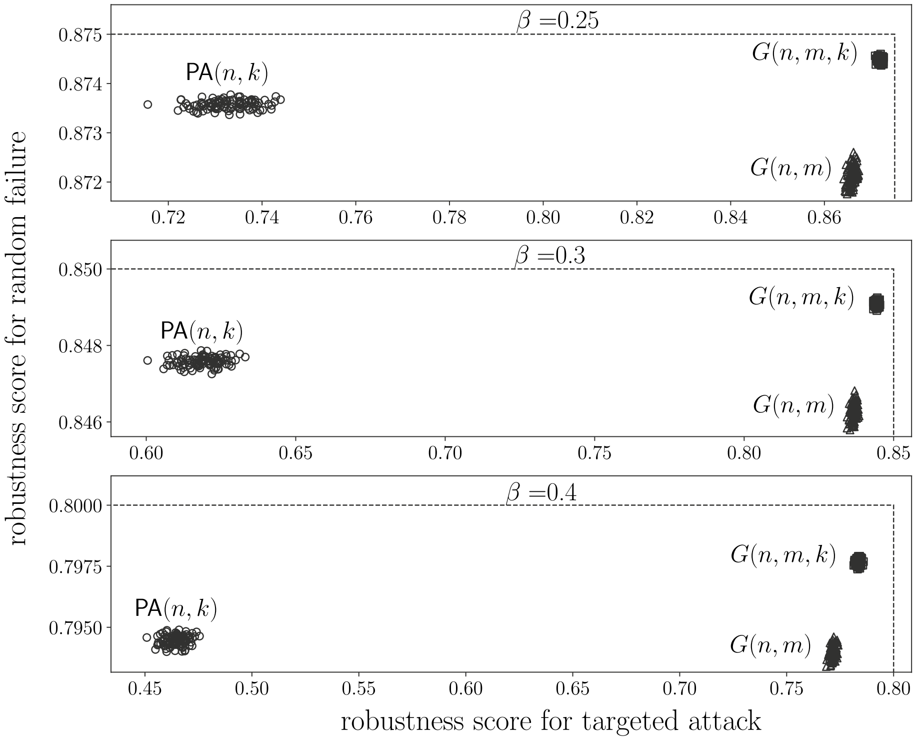

**Fig. 2** Robustness of networks generated from PA$(n, k)$ compared to networks drawn from G$(n, m)$ and G$(n, m, k)$ after 25%, 30% and 40% of vertices were removed in targeted attacks or random failures, where $n = 10{,}000$, $m = 30{,}000$, and $k = 3$. The dashed lines represent the upper bounds for the robustness score as given in "Network robustness" section

### Sensitivity to the choice of parameters in the PA model

Here, we evaluate the sensitivity of the patterns inferred based on Figs. 1 and 2, to the variation of parameters $n$ and $k$ in the underlying preferential attachment model PA$(n, k)$. To this end, we vary $k \in \{3, 4, 5\}$ for fixed $n = 10{,}000$ and $n \in \{1000, 10{,}000, 20{,}000\}$ for fixed $k = 3$, all else being equal and precisely as in the setting presented at the beginning of "Experiments" section.

For each pair of $n$ and $k$ considered, we use $z$-scores to compare the networks generated from PA$(n, k)$ with random networks drawn from G$(n, m)$ and random networks drawn from G$(n, m, k)$, where $m = nk$.[3] The comparison refers to their expected robustness score when $\beta \in \{0.05, 0.1, 0.2, 0.25, 0.3, 0.4\}$ fraction of vertices are removed under targeted attacks or random failures. The obtained $z$-scores are visualized in Fig. 3. Our results suggest that networks generated by using preferential attachment are consistently more robust against random failures but more fragile against targeted attacks when compared to random networks of the same size. This is underscored by the fact that the points corresponding to the latter networks are located in the fourth quadrants in Fig. 3. However, we note that preferential-attachment networks are always more vulnerable to targeted attacks and random failures when compared to random networks of the same

[3] Given a group $X$ and a reference group $Y$, both of size $N$, with respective means $\mu_X, \mu_Y$ and standard deviations $\sigma_X, \sigma_Y$, we compute the corresponding $z$-score as $\sqrt{N}(\mu_X - \mu_Y)/(\sqrt{\sigma_X^2 + \sigma_Y^2})$. Its positive and negative values represent a tendency of elements in $X$ to reach values above and below the reference mean $\mu_Y$, respectively.

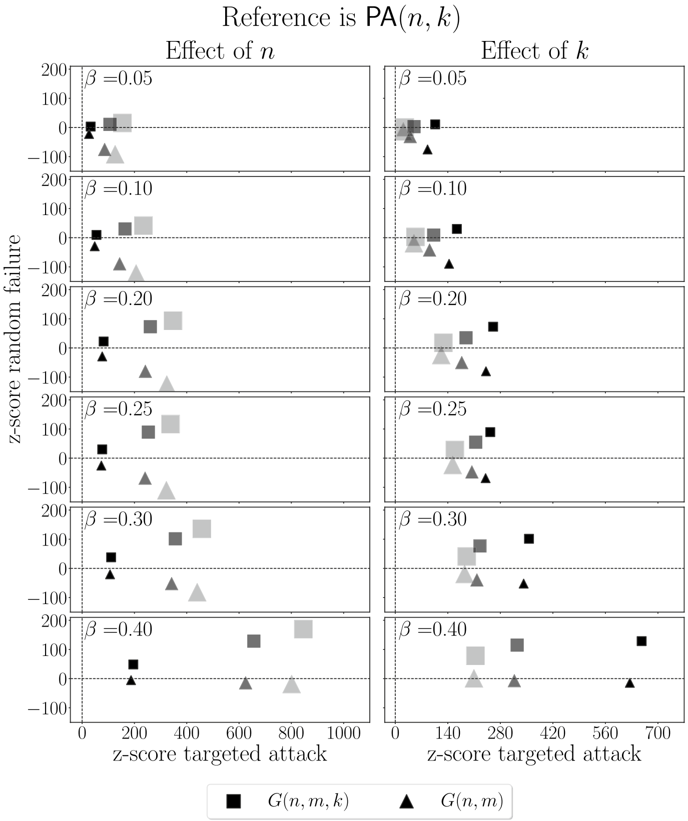

**Fig. 3** In the column on the left, the larger marker sizes correspond to the larger values of $n \in \{1000, 10{,}000, 20{,}000\}$ for fixed $k = 3$. In the column on the right, the larger marker sizes correspond to the larger values of $k \in \{3, 4, 5\}$ for fixed $n = 10{,}000$

size whose minimum degree is at least as large. This is underscored by the fact that the points corresponding to the latter networks are located in the first quadrants in Fig. 3. We note that our claimed patterns hold for varying $n$ or $k$, however, the patterns we assert become more significant as $n$ increases and less significant as $k$ increases. In other words, the patterns we discuss are most evident for larger and sparser networks, which are generally of greater relevance.

## Sensitivity to the choice of the instances

In Figs. 1 and 2, the cohesion of points belonging to the same network type and their separation from points corresponding to other network types can be observed for any fixed proportion of removed vertices $\beta \in \{0.05, 0.1, 0.2, 0.25, 0.3, 0.4\}$. This observation suggests that the patterns inferred from these figures do not depend on a particular choice of instances from the underlying network models. To measure this quantitatively, we compute a silhouette score for each fixed $\beta$ using the Euclidean distance metric by assigning scattered points of each specific type of network to a group.[4] The computed silhouette scores are presented in Table 1.

[4] Given a set of objects, each assigned to a group, and a distance metric defined between all pairs of these objects, the silhouette score measures the similarity of an object to its group (cohesion) compared to other groups (separation) (Rousseeuw 1987). This score ranges from −1 to +1, with higher scores indicating that the data are well clustered and lower scores indicating that the data are poorly clustered.

**Table 1** Silhouette scores corresponding to network clusters in Figs. 1 and 2

| $n = 10{,}000, k = 3$ | $\beta = 0.05$ | $\beta = 0.1$ | $\beta = 0.2$ | $\beta = 0.25$ | $\beta = 0.3$ | $\beta = 0.4$ |
|---|---|---|---|---|---|---|
| | 0.840 | 0.882 | 0.910 | 0.915 | 0.924 | 0.930 |

**Table 2** For each fixed combination of $n$ and $k$, we generate three clusters of networks, as described at the beginning of "Experiments" section. Then, for each fixed $\beta \in \{0.05, 0.1, 0.2, 0.25, 0.3, 0.4\}$, we compute a silhouette score for the three corresponding groups, using the same procedure that we used to obtain the values in Table 1

| **Effect of** $n, \beta$ | $k = 3$ | | |
|---|---|---|---|
| | $n = 1000$ | $n = 10{,}000$ | $n = 20{,}000$ |
| (a) Fixed $k$ and varying $n, \beta$ | | | |
| $\beta = 0.05$ | 0.498 | 0.840 | **0.891** |
| $\beta = 0.10$ | 0.632 | 0.882 | **0.919** |
| $\beta = 0.20$ | 0.719 | 0.910 | **0.939** |
| $\beta = 0.25$ | 0.720 | 0.915 | **0.940** |
| $\beta = 0.30$ | 0.734 | 0.924 | **0.944** |
| $\beta = 0.40$ | 0.738 | 0.930 | **0.946** |
| **Effect of** $k, \beta$ | $n = 10{,}000$ | | |
| | $k = 3$ | $k = 4$ | $k = 5$ |
| (b) Fixed $n$ and varying $k, \beta$ | | | |
| $\beta = 0.05$ | **0.840** | 0.665 | 0.374 |
| $\beta = 0.10$ | **0.882** | 0.788 | 0.573 |
| $\beta = 0.20$ | **0.910** | 0.851 | 0.717 |
| $\beta = 0.25$ | **0.915** | 0.871 | 0.755 |
| $\beta = 0.30$ | **0.924** | 0.882 | 0.787 |
| $\beta = 0.40$ | **0.930** | 0.889 | 0.832 |

These scores indicate how well instances of the same network type are clustered and how well these clusters separate based on their robustness scores when the networks contained in each cluster are subjected to targeted attacks or random failures. From the results in Table 1, we can observe that the distinction of the network clusters considered with respect to their robustness is consistently high and is not particularly affected by the choice of specific instances. To assess the sensitivity of these observation to changes in the parameters of the underlying preferential attachment model $\mathsf{PA}(n, k)$, we vary $k \in \{3, 4, 5\}$ for a fixed $n = 10{,}000$ and vary $n \in \{1000, 10{,}000, 20{,}000\}$ for a fixed $k = 3$, all else being the same. We give in Table 2 for each $\beta \in \{0.05, 0.1, 0.2, 0.25, 0.3, 0.4\}$ the corresponding silhouette scores. As highlighted by the bold values in Table 2, the cohesion within each group and the separation between different groups increase with $n$ and decrease with $k$ when the underlying preferential-attachment networks are instances of $\mathsf{PA}(n, k)$. This implies that the distinction in robustness between the different network types that we consider becomes more apparent when the focus is on larger and sparser networks.

Furthermore, Tables 1 and 2, indicate that for each fixed combination of $n$ and $k$, the corresponding silhouette scores increase with the fraction of removed vertices $\beta$.

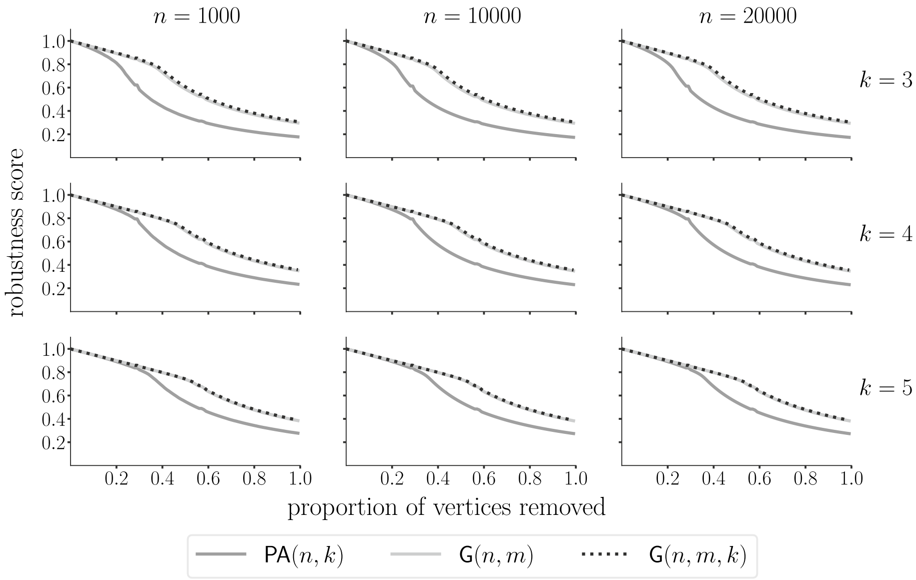

**Fig. 4** The expected robustness score of networks when $\beta \in \{0, 0.01, \ldots, 0.99, 1\}$ fraction of the vertices are removed by adaptive targeted attacks. Here, we consider $m = nk$ for each fixed pair of $n$ and $k$ where $n \in \{1000, 10{,}000, 20{,}000\}$ and $k \in \{3, 4, 5\}$

This means that as the fraction of removed vertices increases, the results become less dependent on a particular choice of network instances.

## Sensitivity to adaptive targeted attacks

In this section, we investigate whether the patterns observed in Figs. 1 and 2 remain consistent under adaptive targeted attacks. In these attacks, the vertices with the highest current degree are removed first, rather than those with the highest initial degree. Such attacks were proposed in Broder et al. (2000) and have been shown to be more effective in dismantling networks than those based on initial degree (Holme et al. 2002; Wu and Holme 2011). To this end, we consider nine combinations of $n$ and $k$ with $n \in \{1000, 10{,}000, 20{,}000\}$ and $k \in \{3, 4, 5\}$, and draw 100 networks from each of the $\mathsf{PA}(n, k)$, $\mathsf{G}(n, m)$, and $\mathsf{G}(n, m, k)$ models, where $m = nk$.

Figure 4 reports the average robustness score (over 100 instances) for each network model when the $\beta \in \{0.01, 0.02, \ldots, 0.99\}$ portion of the vertices are removed in adaptive targeted attacks. We observe that the networks drawn from $\mathsf{G}(n, m)$ and $\mathsf{G}(n, m, k)$ are very similar in terms of their robustness against adaptive targeted attacks. Moreover, we observe that the networks drawn from these two models are noticeably more robust than those generated from $\mathsf{PA}(n, k)$. However, note that this differentiation in robustness does not depend appreciably on $n$ but becomes apparent sooner (i.e., for a lower fraction of vertices removed) when the average degree of the generated graphs is lower (i.e., when $k$ is smaller).

In general, we can conclude that the patterns claimed based on the observations made in Figs. 1 and 2 are consistent under adaptive targeted attacks.

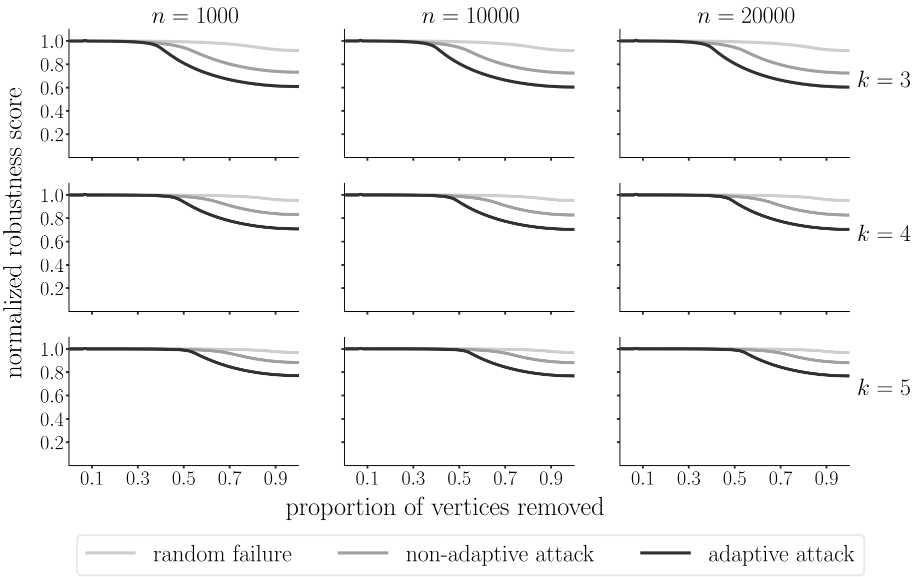

**Fig. 5** The expected robustness score of networks drawn from $\mathsf{G}(n, m, k)$ normalized by the maximum achievable robustness score when $\beta \in \{0, 0.01, \ldots, 0.99, 1\}$ fraction of the vertices are removed by adaptive targeted attacks, non-adaptive targeted attacks, or random failures. Here, we consider $m = nk$ for each fixed pair of $n$ and $k$ where $n \in \{1000, 10{,}000, 20{,}000\}$ and $k \in \{3, 4, 5\}$

### Consistency of near-optimal robustness

In our experiments, we have used networks drawn from $\mathsf{G}(n, m, k)$, where $m = nk$. For $n = 10{,}000, k = 3$, we have seen in Figs. 1 and 2 that these networks exhibit near-optimal robustness against non-adaptive targeted attacks based on initial degree and random failures when only a moderate fraction of their vertices are removed. Here, we evaluate the sensitivity of this pattern to adaptive targeted attacks based on the current degree and its sensitivity to variations in $n$, $k$, and $\beta$. To this end, we consider nine combinations of $n$ and $k$ with $n \in \{1000, 10{,}000, 20{,}000\}$ and $k \in \{3, 4, 5\}$. Then we draw 100 networks from $\mathsf{G}(n, m, k)$ and compute their average robustness score normalized to the maximum achievable robustness score when $\beta \in \{0, 0.01, \ldots, 0.99, 1\}$ portion of the vertices are removed under adaptive targeted attacks, non-adaptive targeted attacks, or random failures.[5] The result is shown in Fig. 5.

When not more than 30% of the vertices are removed by targeted attacks or random failures, Fig. 5 illustrates the consistent near-optimal robustness of the networks drawn from $\mathsf{G}(n, m, k)$ in the case $m = nk$ for a constant $k \geq 3$. We can see that this 30% threshold does not depend appreciably on $n$ but increases with $k$. For example, when $k = 5$, we see across different $n$ that the robustness score does not noticeably deviate from its optimal value when no more than 50% of vertices are removed in targeted attacks or random failures.

From the discussions here, we can conclude that for a constant $k \geq 3$ and $m = nk$, the near-optimal robustness of networks drawn from $\mathsf{G}(n, m, k)$ is consistent as long as the fraction of vertices removed by targeted attacks or random failures is not too large.

[5] Note that for any connected graph, the maximum achievable robustness score after removing $\beta$ portion of the vertices is $1 - \beta/2 + o(1)$, as given in "Network robustness" section.

As a side observation, we can also see that the difference between adaptive and non-adaptive targeted attacks in dismantling the graphs drawn from $\mathsf{G}(n, nk, k)$ becomes apparent only for higher fractions of removed vertices and becomes more pronounced as $k$ increases, but does not depend appreciably on $n$.

Figure 5 shows that, for each considered vertex removal strategy, there is a distinct threshold value $\beta^*$ for the fraction of removed vertices $\beta$, at which the robustness of networks drawn from $\mathsf{G}(n, nk, k)$ deviates considerably from the optimal value. Upon closer investigation, we realized that this threshold corresponds to the point where the second-largest connected component attains its maximum size during the vertex removal process. Specifically, for $\beta < \beta^*$, the size of the second-largest connected component generally increases, while it starts to decrease for $\beta > \beta^*$. At $\beta = \beta^*$, it is noteworthy that the graph's average degree is strictly less than two, and its $k$-core is empty for all $k \geq 3$. This implies that the graph is 2-degenerate, meaning the maximum degree in every induced subgraph is at most 2.

It is desirable to establish a lower bound for $\beta^*$ that is independent of the chosen vertex removal strategy. To this end, note that the robustness and density of graphs drawn from $\mathsf{G}(n, m, k)$ increase with $m$ for fixed $n$ and $k$. Therefore, random $k$-regular ones are the least robust and least dense of such graphs where $m$ attains its minimum possible value of $\frac{1}{2}kn$. For $k \geq 3$, it has been shown that an optimal attacker must remove at least a fraction $\frac{k-2}{2k-2}$ of all vertices to partition a random $k$-regular graph into connected components of sublinear size (see "Bounds on optimal attacks" in Balashov et al. 2019). As a result, for graphs drawn from $\mathsf{G}(n, m, k)$, we can conclude that $\beta^* \geq \frac{k-2}{2k-2}$ when $k \geq 3$, regardless of the vertex removal strategy employed.

## Preferentiality and robustness

In this section, we aim to experimentally investigate how preference in attachment affects the robustness of incrementally constructed networks which inherently have a minimum degree of at least $k$, such as those generated by the preferential attachment model $\mathsf{PA}(n, k)$. To isolate the effects of preference in attachment, we also explore the similar $\mathsf{UA}(n, k)$ model where newly added vertices connect to $k$ existing vertices selected uniformly at random, without a preference for highly connected vertices. Since both $\mathsf{PA}(n, k)$ and $\mathsf{UA}(n, k)$ networks belong to $G(n,\ m,\ k)$ where $m = nk$, we also compare them with typical members of this class using the $\mathsf{G}(n, m, k)$ model.

In our experiments, we vary $n \in \{1000, 10{,}000, 20{,}000\}$ for a fixed $k = 3$, and $k \in \{3, 4, 5\}$ for a fixed $n = 10{,}000$. For each fixed pair of $n$ and $k$, we draw 100 instances from the following network models: $\mathsf{UA}(n, k)$, $\mathsf{PA}(n, k)$, and $\mathsf{G}(n, m, k)$; where $m = nk$. For each fixed pair of $n$ and $k$, we then compare the robustness of the corresponding generated networks against targeted attacks based on the initial degree and random failures when $\beta \in \{0.05, 0.1, 0.2, 0.25, 0.3, 0.4\}$ fraction of the vertices are removed. For this purpose, we used $z$-scores as described in "Sensitivity to the choice of parameters in the PA model" section.

The results depicted in Fig. 6 indicate that $\mathsf{UA}(n, k)$ graphs are consistently more robust under both targeted attacks and random failures than $\mathsf{PA}(n, k)$ graphs, but more fragile than $\mathsf{G}(n, m, k)$ graphs where $m = nk$. We also observe that as $n$ increases, this

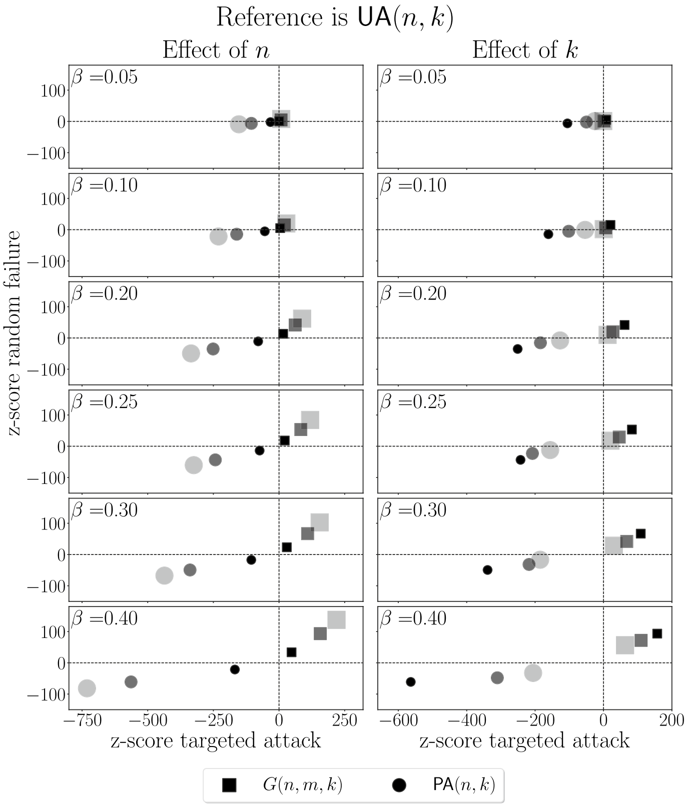

**Fig. 6** In the column on the left, the larger marker sizes correspond to the larger values of $n \in \{1000, 10{,}000, 20{,}000\}$ for fixed $k = 3$. In the column on the right, the larger marker sizes correspond to the larger values of $k \in \{3, 4, 5\}$ for fixed $n = 10{,}000$

pattern becomes more pronounced for a fixed fraction of removed vertices $\beta$, while it diminishes as $k$ increases. Therefore, we can conclude that this trend is particularly applicable to larger and sparser networks. Notably, our findings indicate that a preference for attachment to well-connected vertices in network growth models does not enhance network robustness, but in fact, affects it adversely.

## Conclusions

We have shown that, for any constant $k \geq 3$, almost all graphs in which the number of edges is linear in the number of vertices (i.e., the average degree is upper-bounded by a constant) and the minimum degree is at least $k$, are connected and provably robust against any vertex removal strategy.

Motivated by this new theoretical result, we have shown experimentally that the dictum "robust-yet-fragile" is not a fitting characterization of preferential-attachment networks, let alone scale-free networks in general, because it stems from a poorly chosen baseline. It appears that the previously assessed robustness is largely due to their constant minimum degree, rather than their skewed degree distribution.

Furthermore, we have shown that in the context of network growth models, any preference for attachment to well-connected vertices does not confer an advantage in terms of robustness against random failures or targeted attacks.

Our results show, contrary to the common belief, that preferential attachment graphs are not particularly robust against random failures. What robustness they have is a consequence of a lower-bounded minimum degree, which is guaranteed by the attachment process. The skewed degree distribution obtained from preferential attachment is not strengthening robustness but, in fact, reducing it when compared to uniformly random attachment.

**Acknowledgements**
Not applicable.

**Author contributions**
All authors contributed to the research design, the theoretical results, and the writing of the manuscript. RH conducted the experiments and generated the figures. Both authors read and approved the final manuscript.

**Funding**
Open access funding provided by Swiss Federal Institute of Technology Zurich

**Availability of data and materials**
The generated data and software code are publicly available in the GitHub repository: https://github.com/RouzbehHasheminezhad/ANS-Robustness-PA

## Declarations

**Competing interests**
The authors declare that they have no competing interests.

Received: 28 February 2023 Accepted: 28 May 2023
Published online: 13 June 2023

### References

Albert R, Jeong H, Barabási AL (2000) Error and attack tolerance of complex networks. Nature 406(6794):378–382
Anastos M, Frieze A (2020) Hamilton cycles in random graphs with minimum degree at least 3: An improved analysis. Random Struct Algorithms 57(4):865–878
Balashov N, Cohen R, Haber A, Krivelevich M, Haber S (2019) Optimal shattering of complex networks. Appl Netw Sci 4(1):99
Barabási AL, Albert R (1999) Emergence of scaling in random networks. Science 286(5439):509–512
Batagelj V, Brandes U (2005) Efficient generation of large random networks. Phys Rev E 71(3):036113
Batagelj V, Zaveršnik M (2011) Fast algorithms for determining (generalized) core groups in social networks. Adv Data Anal Classif 5(2):129–145
Benjamini I, Kozma G, Wormald N (2014) The mixing time of the giant component of a random graph. Random Struct Algorithms 45(3):383–407
Bollobás B (1980) A probabilistic proof of an asymptotic formula for the number of labelled regular graphs. Eur J Comb 1(4):311–316
Bollobás B, Cooper C, Fenner TI, Frieze AM (2000) Edge disjoint Hamilton cycles in sparse random graphs of minimum degree at least $k$. J Graph Theory 34(1):42–59
Broder A, Kumar R, Maghoul F, Raghavan P, Rajagopalan S, Stata R et al (2000) Graph structure in the web. Comput Netw 33(1):309–320
Doyle JC, Alderson DL, Li L, Low S, Roughan M, Shalunov S et al (2005) The robust yet fragile nature of the Internet. Proc Natl Acad Sci 102(41):14497–14502
Erdős P, Rényi A (1959) On random graphs I. Publ Math Debr 6:290–297
Friedman L, Krivelevich M (2021) Cycle lengths in expanding graphs. Combinatorica 41(1):53–74
Giakkoupis G, Sauerwald T (2012) Rumor Spreading and Vertex Expansion. In: Proceedings of the 2012 annual ACM-SIAM symposium on discrete algorithms (SODA). Proceedings. Society for Industrial and Applied Mathematics, pp 1623–1641
Hasheminezhad R, Brandes U (2022) Constructing Provably Robust Scale-Free Networks. In: Ribeiro P, Silva F, Mendes JF, Laureano R (eds) Proceedings of the 7th international winter conference on network science (NetSci-X 2022), vol. 13197 of lecture notes in computer science. Springer, Cham, pp 126–139
Hasheminezhad R, Brandes U (2023) Robustness of preferential-attachment graphs: shifting the baseline. In: Cherifi H, Mantegna RN, Rocha LM, Cherifi C, Micciche S (eds) Complex networks and their applications XI. Studies in computational intelligence. Springer, Berlin, pp 445–456
Hasheminezhad R, Boudourides M, Brandes U (2020) Scale-free networks need not be fragile. In: Proceedings of the 2020 IEEE/ACM international conference on advances in social networks analysis and mining (ASONAM 2020). IEEE, The Hague, pp 332–339
Holme P, Kim BJ, Yoon CN, Han SK (2002) Attack vulnerability of complex networks. Phys Rev E 65(5):056109

Janson S, Luczak MJ (2008) Asymptotic normality of the *k*-core in random graphs. Ann Appl Probab 18(3):1085–1137

Klau GW, Weiskircher R (2005) Robustness and resilience. In: Brandes U, Erlebach T (eds) Network analysis. Volume 3418 of lecture notes in computer science. Springer, Berlin, pp 417–437

Molloy M, Reed B (1998) The size of the giant component of a random graph with a given degree sequence. Comb Probab Comput 7(3):295–305

Petersen C, Rotbart N, Simonsen JG, Wulff-Nilsen C (2016) Near optimal adjacency labeling schemes for power-law graphs. In: Chatzigiannakis I, Mitzenmacher M, Rabani Y, Sangiorgi D (eds) Proceedings of the 43rd international colloquium on automata, languages, and programming (ICALP 2016). vol 55 of Leibniz international proceedings in informatics. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, pp 133:1–133:15

Rousseeuw PJ (1987) Silhouettes: a graphical aid to the interpretation and validation of cluster analysis. J Comput Appl Math 20:53–65

Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ (2011) Mitigation of malicious attacks on networks. Proc Natl Acad Sci 108(10):3838–3841

Wu ZX, Holme P (2011) Onion structure and network robustness. Phys Rev E 84(2):026106

## Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.