Scale-free networks need not be fragile

Rouzbeh Hasheminezhad
Social Networks Lab
ETH Zürich
Zürich, Switzerland
shashemi@ethz.ch

Moses Boudourides
SPS Master's in Data Science Online Program
Northwestern University
Evanston, IL, U.S.A.
moses.boudourides@northwestern.edu

Ulrik Brandes
Social Networks Lab
ETH Zürich
Zürich, Switzerland
ubrandes@ethz.ch

***Abstract*—We report on computational experiments testing the robustness of scale-free networks. The stylized fact that such networks are robust under random failure but sensitive to targeted attack originates from experiments on instances generated by preferential attachment. We find that these are not representative but rather outliers: they are significantly more fragile under targeted attack than random scale-free networks with the exact same degree sequence. To show that they are, however, not extreme in this respect, we also present two generators producing scale-free networks with the same degree sequence that are even more fragile than the corresponding preferential-attachment networks or more robust than even random graphs. The latter is based on a new result about realizability of scaling degree sequences with a degree-ordered Hamiltonian cycle.**

***Index Terms*—network models, resilience, graph generators**

I. Introduction

A network is robust to the degree that its functions are preserved after parts of its structure have been removed [1]. We focus on the particular case of the largest connected component in scale-free networks after node removal. Two scenarios have been considered in a seminal study [2] comparing scale-free networks to random networks: removal uniformly at random (*random failure*) and removal of nodes with larger degree first (*targeted attack*). The conclusion is that scale-free networks are more robust under random failure but substantially more sensitive to targeted attack. This led to the stylized fact that scale-free networks are characterized by a "robust-yet-fragile" [3] structure.

The initial experiments [2], however, used two empirical networks classified as scale-free and synthetic networks generated from preferential attachment [4]. While the class of scale-free networks (characterized by their degree sequences) and preferential-attachment networks (defined by a generative model) are often treated as if synonymous, bounds on the lengths of adjacency-labeling schemes show that the latter are but a tiny subset of the former [5]. It is therefore open whether the characterization of scale-free networks as robust-yet-fragile is actually specific to preferential-attachment networks.

We conduct a small series of experiments comparing the robustness of preferential-attachment networks to that of the most similar scale-free networks (i.e., those with the same degree sequence) and find that preferential-attachment networks actually are outliers in terms of their sensitivity to targeted attack. They are, however, not extreme because we can construct even more fragile networks from the same degree sequences. While overall scale-free networks conditioned on preferential-attachment degree sequences are indeed more fragile than random networks, we also show how to construct instances that are significantly more robust than their random counterparts.

II. Preliminaries

For the purpose of this paper, we consider only networks that are represented as simple undirected graphs, and use both terms interchangeably.

A. Graphs and degree sequences

We consider simple undirected graphs $G = (V, E)$ where V is the set of vertices, or nodes, and $E \subseteq \binom{V}{2}$ is the set of edges, or links. We generally denote $n = n(G) = |V|$ and $m = m(G) = |E|$. The *degree* of a vertex $v \in V$ is the number $\deg(v) = |\{w \in V : \{v, w\} \in E\}|$ of its *neighbors*. If the vertices are ordered $v_1, \ldots, v_n$ such that $\deg(v_1) \geq \cdots \geq \deg(v_n)$, then $D(G) = (\deg(v_1), \ldots, \deg(v_n))$ is the *degree sequence* of G. A sequence $D = (d_1, \ldots, d_n)$ of integers is called *graphical*, if $n > d_1 \geq \cdots \geq d_n \geq 0$ and there is a simple undirected graph with $D = D(G)$. The graph is then said to *realize* the sequence, and we denote by $G(D)$ the set of all realizations of D. Let $\hat{G}(D) \subseteq G(D)$ be the subset of connected graphs, then D is called *potentially connected*, if $\hat{G}(D) \neq \emptyset$.

An integer sequence $D = (d_1, \ldots, d_n)$ is called *scaling*, if degrees follow a *power law* $k = c \cdot d_k^{-\gamma}$ for $k = 1, \ldots, n$ and constants c and $\gamma > 0$ [6]. Constant γ is called its *scaling factor*. A graph with a scaling degree sequence (up to some tolerance) is called *scale free*. Note that we adopt a non-stochastic treatment because we are interested in the degree sequences of particular graphs.

One of several statistics linking degrees with the structure of the graph is *degree assortativity* [7], defined as

$$r(G) = \frac{M_2(G) - \frac{M_1(G)^2}{4m}}{\frac{1}{2}\sum\limits_{v \in V} \deg(v)^3 - \frac{M_1(G)^2}{4m}}$$

where $M_1(G) = \sum_{v \in V} \deg(v)^2$ is the first and $M_2(G) = \sum_{\{u,v\} \in E} \deg(u) \deg(v)$ is the second *Zagreb index* [8]. Since $M_2(G)$ is the only term that is not determined by the degree sequence alone, degree assortativity indicates the extent to which adjacent vertices are of like degree.

B. Graph generators

A *(uniform) random graph*, or Erdős-Rényi graph [9], is a graph drawn uniformly at random from the set $G(n, m)$ of all graphs with n vertices and m edges. In slight abuse of notation, we will use $G(n, m)$ for both the set and the model. In a random graph, the distribution of degrees is binomial, and approaches a Poisson distribution for sparse graphs with $m \in O(n)$. Hence, degrees are expected to be sharply concentrated around $2m/n$.

A graph from the set $G(D)$ of graphs realizing a graphical sequence D can be obtained using the algorithm of Havel [10] and Hakimi [11]. Assume we have created vertices $v_1, \ldots, v_n$, then it is usually implemented by (i) linking vertex v_1 to $v_2, \ldots, v_{1+d_1}$ and (ii) recursing on the sequence $d_2-1, \ldots, d_{1+d_1}-1, d_{2+d_1}, \ldots, d_n$ of *residual degrees*. Note, however, that the algorithm also works for any other vertex in step (i), as long as step (ii) links it with the highest degree vertices other than itself [12].

Scale-free graphs are often generated using *preferential attachment* [4]. There are some ambiguities and degrees of freedom in the model [13] that have led to different instantiations. We use models $\mathsf{PA}(n, d)$, $d \ll n$, defined as follows. Starting from a complete graph K_{2d+1}, add $n-(2d+1)$ many vertices one at a time, and link each of them to d vertices drawn without replacement from the pool of already added vertices with probability proportional to their degree so far. This ensures the absence of loops and multiple edges. A total of $n \cdot d$ edges is created, and the expected number of vertices of degree k is in $\Theta(k^{-3})$ [14], i.e., the degree sequence is close to scaling with $\gamma = 2$.[1]

Thus, we can expect the degree sequence of a graph generated by preferential attachment to be scaling. On the other hand, the process generates only a tiny subset of all scale-free graphs. A reversal of the vertex addition sequence shows that the graphs generated according to $\mathsf{PA}(n, d)$ are d-degenerate (i.e., every induced subgraph has a vertex of degree at most d). Results on adjacency labeling exploit this observation to encode preferential-attachment graphs with a number of bits that is asymptotically vanishing compared to a lower bound for scale-free graphs even when the scaling factor is fixed to $\gamma = 2$ [5].

C. Robustness

Two types of damage scenarios for networks are considered [2]. In the *random failure scenario*, nodes are removed uniformly at random, whereas in the *(static) targeted attack scenario*, they are removed in non-increasing order of their original degree. Both scenarios are parameterized with the fraction $\beta \in (0, 1]$ of nodes removed.

While many other criteria for robustness exist [1] we here focus on the part of the graph that remains connected. For a graph G, let $\hat{n}(G)$ be the number of vertices in a largest connected component, or LCC for short. If $B \subseteq V$, $|B| = \lceil \beta n \rceil$, is the set of vertices removed, the relative size of a LCC is

$$\frac{\hat{n}(G[V \setminus B])}{\hat{n}(G)} ,$$

where $G[V \setminus B]$ denotes the subgraph induced by the remaining vertices. Clearly, it is bounded from above by $1 - \beta$ if G is connected. To incorporate the rate at which the giant component breaks apart, rather than just the time at which its relative size falls below a threshold, we consider the average over the entire sequence of removals. Let $b_1, \ldots, b_{|B|}$ be the vertices of B in the order of removal, then we define

$$R_G(B) = \frac{1}{|B|} \sum_{i=1}^{|B|} \frac{\hat{n}(G[V \setminus \{b_1, \ldots, b_i\}])}{\hat{n}(G)}$$

as a generalization of the *robustness index* [15], allowing for removal sequences with $\beta < 1$. The index lies in the range $[\frac{1}{n}, 1 - \frac{\lceil \beta n+1 \rceil}{2n}]$ with the extreme cases attained by the star $K_{1,n-1}$ and the clique K_n.

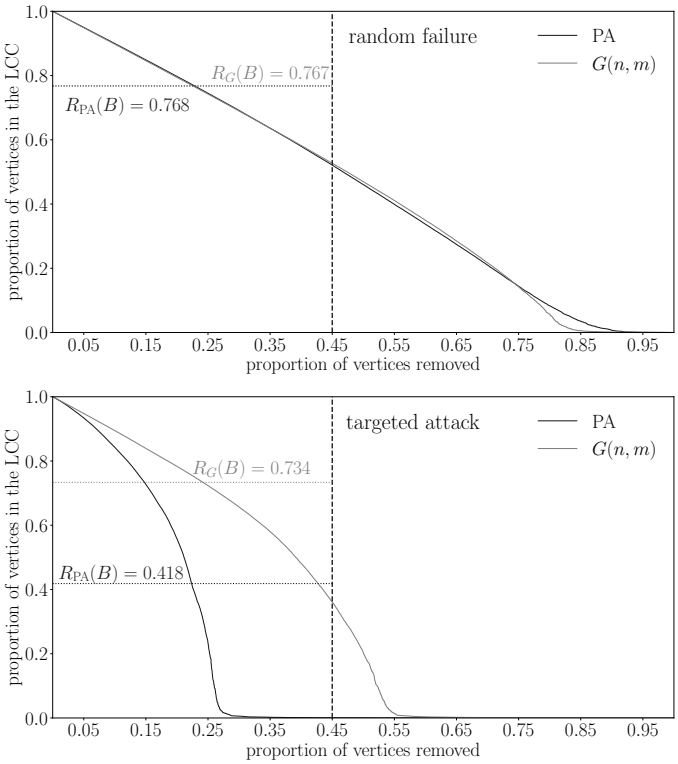

Fig. 1. The relative size of the largest connected component in a preferential-attachment graph and a uniform random graph as a function of the fraction β of vertices removed in both damage scenarios. Both graphs have $n = 10000$ and $m = 30000$ and are initially connected. As expected, the robustness score for $\beta = 0.45$ hardly differs under random failure but is lower for the preferential-attachment graph under targeted attack.

III. Experiments

Our experiments are designed to test whether the robustness of scale-free networks is adequately described by instances

[1] Note that we defined scaling of degree sequences in terms of ranks rather than frequencies, so that the scaling factor is one less than the exponent in the degree distribution [6].

generated from preferential attachment. Because of their particular configuration and relatively small number, we hypothesize that this is not the case.

To be sure, we are rather strict about the scale-free networks we compare with. A scale-free preferential-attachment network is compared only with other scale-free networks that have the exact same degree sequence. In addition to randomly sampled scale-free networks, two rather extreme types of networks are generated as described in the following subsection.

A. Graphs with fixed degree sequence

Any graphical sequence D can be realized using the Havel-Hakimi algorithm from Sec. II. Standard implementations pick a vertex of maximum degree in each step, but to create graphs with low degree assortativity, we introduce a variant, *smallest-first Havel-Hakimi* (sfH^2), in which the vertex chosen next is of minimum degree. This has the added advantage that the graphs are also (maximally) connected.

Theorem 1: [16] Given a potentially connected graphical sequence D, sfH^2 realizes a connected graph with maximum connectivity[2] in $\hat{G}(D)$.

Since all neighbors of low-degree vertices are among the vertices of highest degree, graphs generated by sfH^2 are especially sensitive to targeted attack.

To generate graphs that are almost perfectly robust, we plant a Hamiltonian cycle (i.e., a simple cycle containing all vertices) on which vertices appear in order of their degrees. If vertices are removed in the same order, the rest of the graph remains connected.

We therefore introduce another variant, *Hamiltonian Havel-Hakimi* (H^3), that first creates a Hamiltonian cycle on vertices $v_1, \ldots, v_n$ and then iteratively connects a vertex to those of highest residual degree that are not its neighbors on the cycle. Note that there is ambiguity in the order in which vertices of the same degree are removed in a targeted attack. To safeguard against systematic effects we introduce a specialization, *randomized Hamiltonian Havel-Hakimi* (rH^3), that randomizes both, the order in which equal-degree vertices appear in the cycle, and the rule by which ties are broken among residual degrees.

The H^3 algorithm cannot realize every graphical sequence, because not every potentially connected graphical sequence admits a Hamiltonian realization. However, due to a recent result in degree-based graph construction (Theorem 6 in [17]), the algorithm can realize any potentially connected graphical sequence that admits a Hamiltonian realization. Therefore, the following result provides confidence that any graphical sequence that is close enough to scaling can be realized with a degree-ordered Hamiltonian cycle using any variant of H^3 including rH^3. The proof is in the appendix.

Our experience is that the algorithm realizes graphical sequences even if they are only approximately scale-free.

[2]The connectivity of a graph is the largest k for which the graph is k-connected. A connected graph is said to be k-connected if it has more than k nodes and remains connected whenever fewer than k nodes are removed.

Theorem 2: For sufficiently large n, any graphical sequence that is scaling with a factor $\gamma > 1$ and has bounded minimum degree at least 2, admits a Hamiltonian realization.

Whereas a minimum degree bounded by a constant d is no restriction in the context of preferential attachment, random graphs with $d \cdot n$ edges are disconnected with high probability [18]. For the network-size regime we consider in our experiments, random graphs matching the size of preferential-attachment networks with minimum degree $d \geq 3$ still tend to have almost all of their nodes in the largest connected component, but this is not the case for $d = 2$. Moreover, minimum degree two requires the following special handling when attempting to realize robust networks using rH^3.

Given a graphical sequence $D = (d_1, \ldots, d_n)$ with minimum degree $d_n = 2$, let k be the largest index such that $d_{n-k+1} = \ldots = d_n = 2$. Applied to this sequence, rH^3 yields a graph in which the planted Hamiltonian cycle contains an induced path P_k of k vertices. It is therefore highly sensitive to vertex deletions, since the removal of any pair of vertices in P_k detaches the entire subpath between them.

To mitigate this problem, rH^3 is applied to the sequence $d_1, \ldots, d_{n-k}$. Afterwards, select k edges not on the Hamiltonian cycle and introduce k additional vertices by subdividing them.

B. Instance creation

The seminal experiments of Albert et al. [2] used two kinds of data, two empirical networks classified as scale-free, and graphs generated from $\mathsf{PA}(n, 2)$ with $n \in \{1000, 5000, 10000, 20000\}$ for comparison with uniform random graphs. Only the results for one pair of graphs with $n = 10000$ are presented in detail, and removal fractions of $\beta \in \{0.05, 0.18, 0.45\}$ are used in an illustration of different stages of damage.

In all our experiments, we start by generating graphs from $\mathsf{PA}(n, d)$ until we obtain one G_{PA} that passes as scale-free according to a standard criterion [19] as implemented in the python-igraph package [20]. Note that graphs from $\mathsf{PA}(n, d)$ are necessarily connected. Let $D = D(G_{\mathsf{PA}})$ be its (scaling, potentially connected) degree sequence.

Next we use sfH^2 and rH^3 to create two special scale-free graphs from $\hat{G}(D)$.

Finally, graphs are drawn uniformly at random from $\hat{G}(D(G_{\mathsf{PA}}))$, i.e., random connected scale-free graphs with the same degree sequence. This can be done, for instance, by starting from any of the three graphs in $\hat{G}(D(G_{\mathsf{PA}}))$ that we already have and performing a series of connectivity-preserving edge swaps [21]. Size-matching random graphs are drawn from $G(n, dn)$ using rejection sampling until they are almost fully connected (95% of nodes in the largest connected component).

We use graph-tool [22] for graph generation and index computations. All robustness scores reported below are averages over ten independently drawn vertex-removal orders.

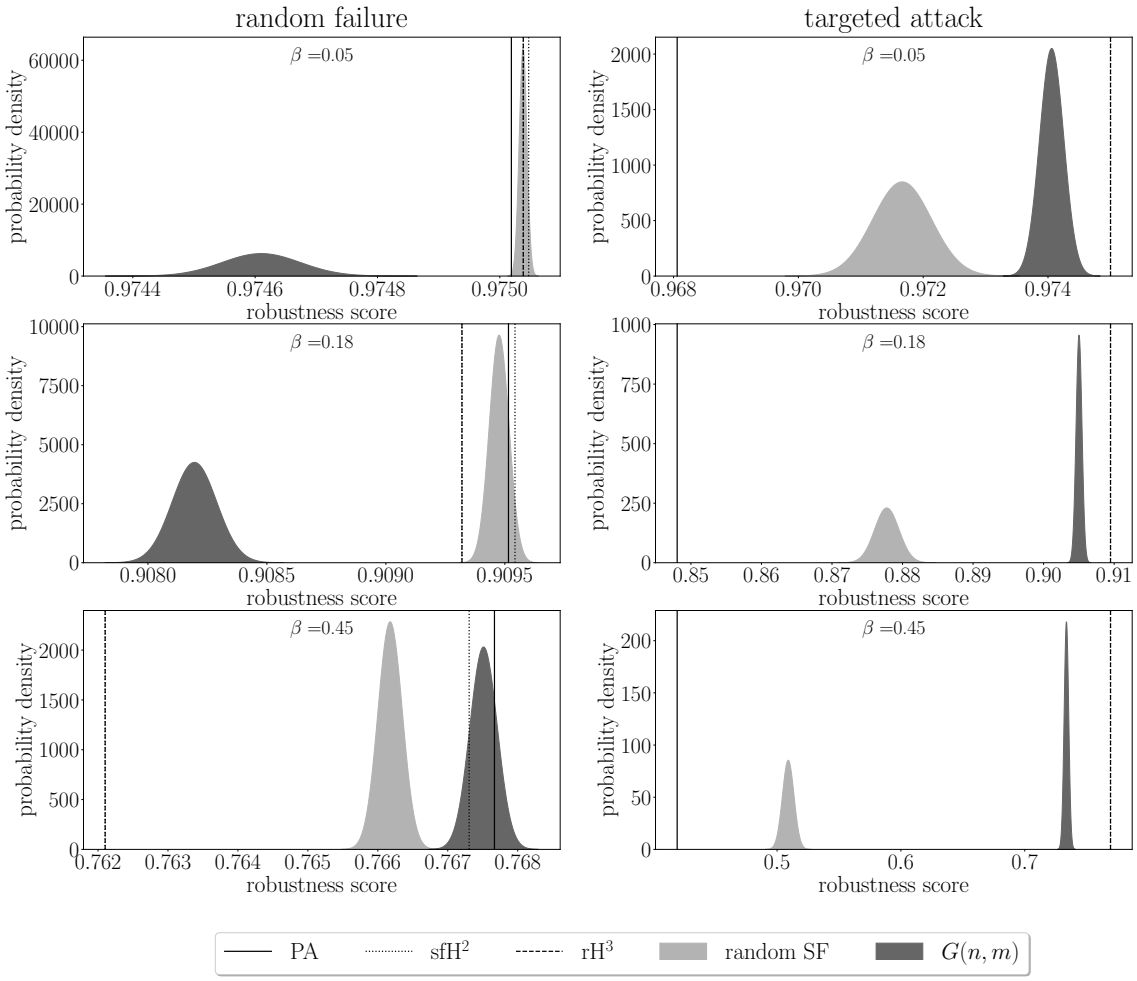

Fig. 2. Robustness of preferential-attachment networks in context. For both damage scenarios (left/right) we show robustness scores after removing 5%, 18%, and 45% of all nodes (top to bottom). The scores of sfH^2 under targeted attack are off the chart for $\beta \in \{0.05, 0.18, 0.45\}$ (at about $0.68, 0.43$ and 0.19). The robustness scores of randomly sampled graphs passed the tests for normality and are therefore shown in stylized form for visual clarity.

C. Preferential attachment is not typical for scale-freeness

In the first experiment, we pit a scale-free preferential-attachment network generated from $\mathsf{PA}(10000, 3)$ against random scale-free networks with the same degree sequence and uniform random graphs of the same size. Note that, for the original setting of $d = 2$ [2], random graphs of the same size are rarely connected.

The results for a typical preferential-attachment network are shown in Fig. 2, where $5\%, 18\%$ and 45% of vertices are removed in both damage scenarios. Since the robustness of random scale-free and uniform random graphs were found to be distributed normally we show stylized normal distributions with sample mean and variance for clarity. To test normality, we used the Kolmogorov-Smirnov test as implemented in the SciPy package [23] with 35 samples and a significance level of 0.05.

Overall, the conclusions of Albert et al. [2] regarding the relationship between the robustness of scale-free and random graphs are largely corroborated. For smaller percentages of removals, $\beta \in \{0.05, 0.18\}$, scale-free networks are significantly more robust than random graphs under random failure (with tiny differences), but significantly more fragile under targeted attack (with larger differences and the exception of rH^3).

Despite showing the same tendencies, however, we find that the preferential-attachment networks differ significantly from random scale-free networks, even when conditioned on the same degree sequence. They are among the most fragile against targeted attacks and therefore exaggerate the relationship between scale-free and random networks.

The instances generated from sfH^2 and rH^3 indicate that even more extreme scale-free networks exist, with the instance from rH^3 being more robust than even random graphs.

D. The distinction is consistent

The second experiment is a repetition of the first, but instead of comparing one network with multiple random samples, we do a paired comparison of multiple networks with single samples.

Ten scale-free networks are generated from $\mathsf{PA}(10000, 3)$ and each of them is paired with a triple of networks that

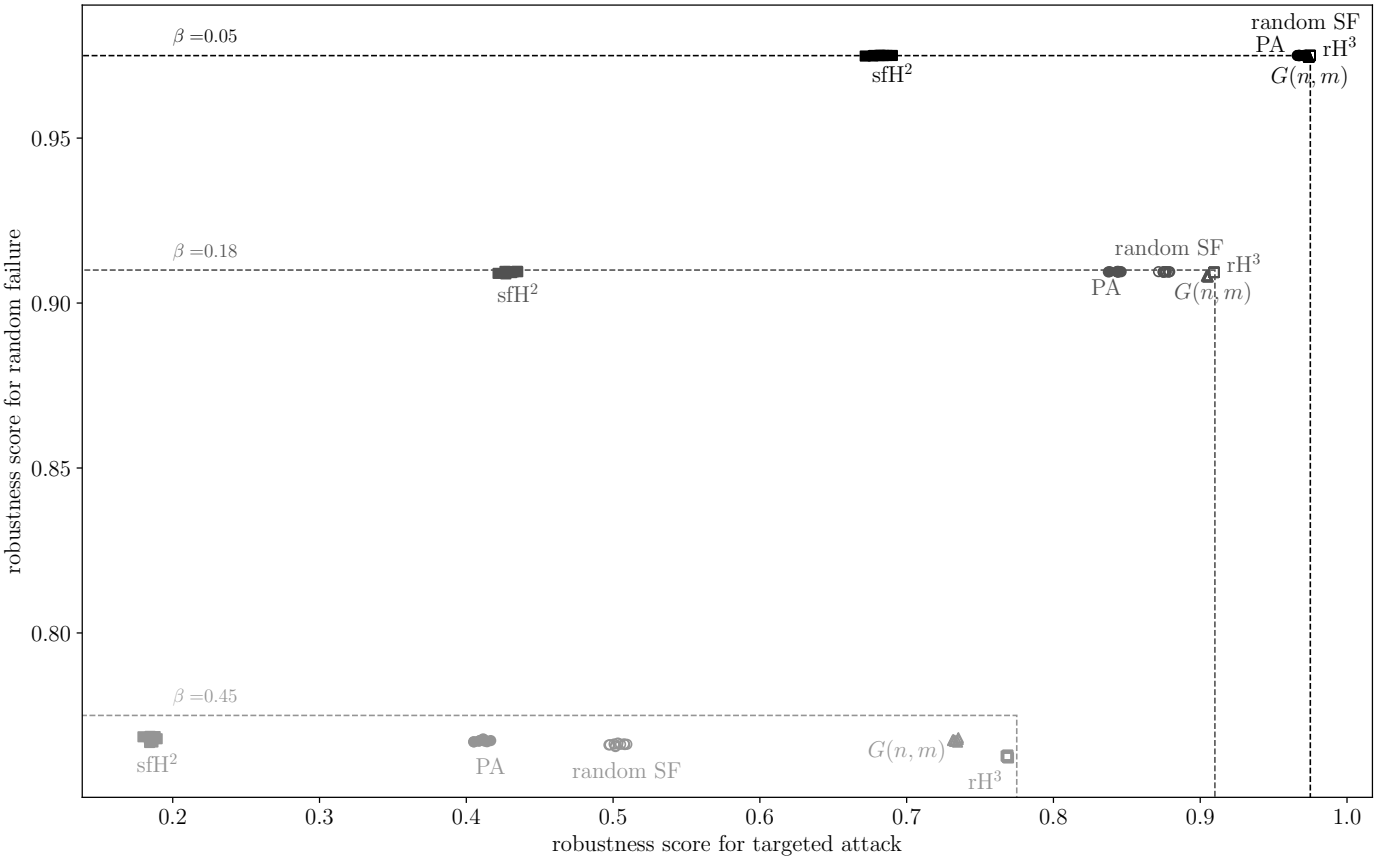

Fig. 3. Robustness for $\beta \in \{0.05, 0.18, 0.45\}$. Dashed lines represent upper bounds of $1 - \frac{\lceil \beta n+1 \rceil}{2n}$ on the robustness scores.

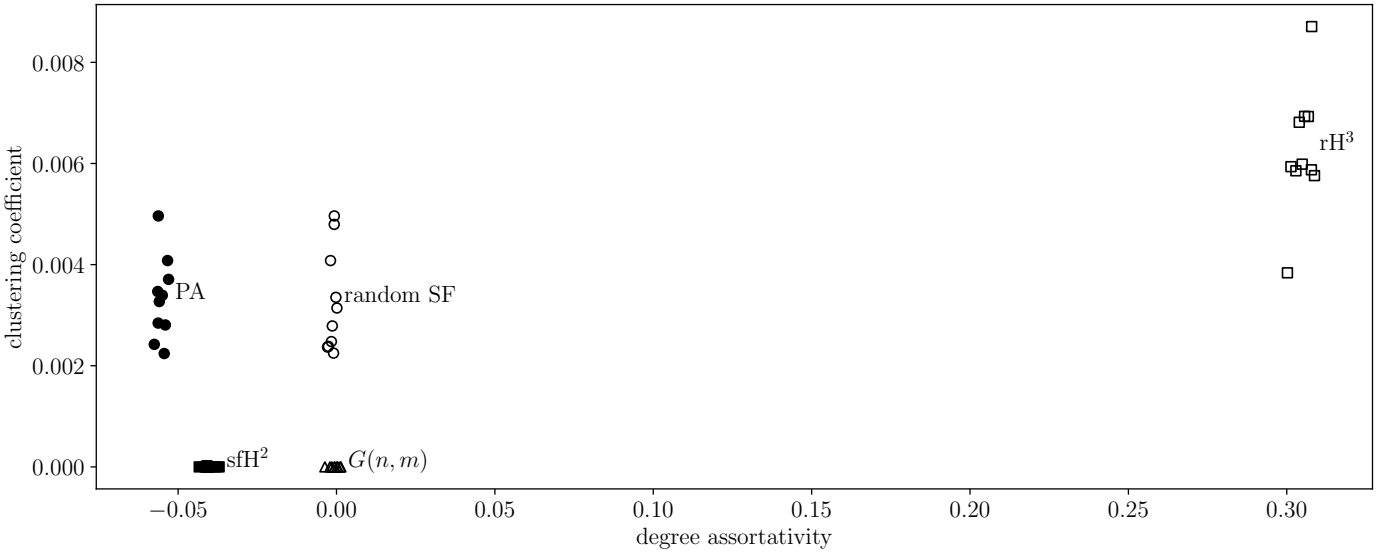

Fig. 4. Degree assortativity vs. clustering coefficient for the same networks as in Fig. 3.

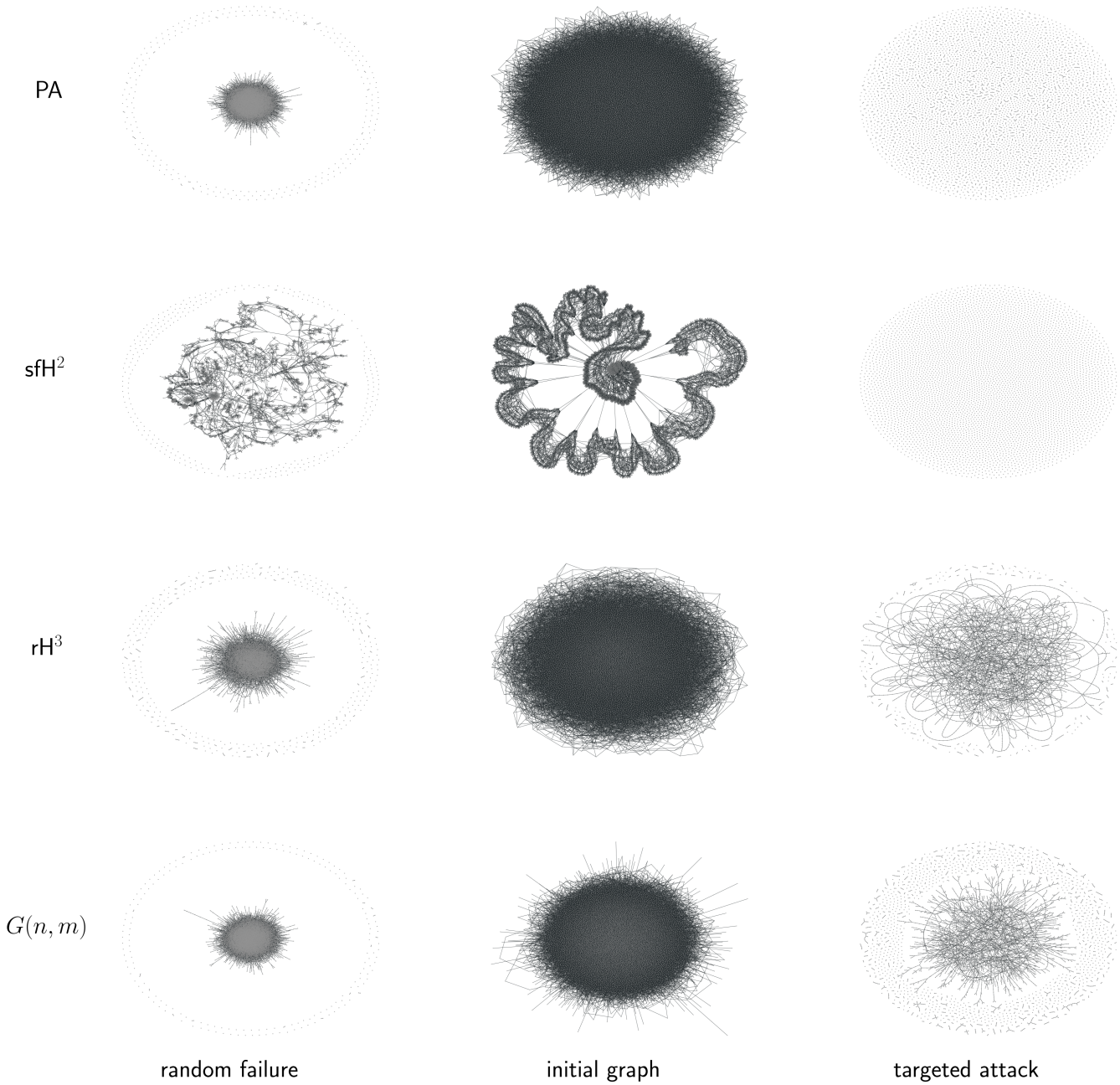

Fig. 5. Illustration of the effects of node removal on actual examples. A preferential-attachment graph is generated from $\mathsf{PA}(10000, 3)$ and two more scale-free graphs with the same degree sequence are obtained from sfH^2 and rH^3; the uniform random graph has the same number of vertices and edges. The outer columns show the graphs remaining after 45% of vertices have been removed.

have the same degree sequence: one connected random scale-free graph, and one each from sfH^2 and rH^3. In addition we generate ten random graphs from $G(10000, 30000)$. Note that similar to Sec. III-B, we use rejection sampling to ensure that the generated preferential-attachment networks pass as scale-free and also to ensure that the generated random graphs are almost fully connected.

In the scatterplot of Fig. 3, graphs from the same generator cluster strongly, and clusters separate increasingly for larger fractions of removed vertices.

All instances are highly robust against random failure but there are stark differences with respect to targeted attacks. The ordering that emerges is clearly visible for $\beta = 0.45$ and suggests that the findings of the first experiment are not dependent on the initial preferential-attachment network.

E. Structural factors

With the final experiment we illustrate possible reasons underlying the observed relationships. For the instances generated in the second experiment, two structural characteristics are plotted in Fig. 4.

It has been pointed out before that degree assortativity (see Sec. II) has an influence on robustness (e.g., [24]). In disassortative networks, lower-degree vertices may be more likely to become detached from the giant component when loosing their higher-degree neighbors during a targeted attack. Unlike preferential-attachment networks, random connected scale-free networks with the same degree sequence do not exhibit disassortativity.

An index measuring local cohesion is the *clustering coefficient*, defined as the density $c(v) = \frac{m(G[N(v)])}{\binom{\deg(v)}{2}}$ of the neighborhood of vertices $v \in V$ with $\deg(v) \geq 2$, and zero otherwise. The clustering coefficient of the graph $C(G)$ is the average $c(v)$ taken over all nodes $v \in V$ [25].

While networks generated by sfH^2 do not have the same level of disassortativity as preferential-attachment networks, their lack of local clustering may be a reason for increased vulnerability. Networks generated with rH^3 are by far the most assortative and locally dense scale-free networks in our study. Fig. 5 exemplifies with specific instances what has been expressed by summary statistics so far.

We add that relative to the other network types considered in this paper, the rH^3 networks are noticeably more connected within the core consisting of high degree nodes and also within the periphery consisting of the other lower degree nodes. This is at the expense of a looser connection between core and periphery.

IV. Conclusion

Scale-free networks are defined by their degree sequence, preferential-attachment networks by a generative model. While the model typically generates scale-free networks, these are special even among those with the exact same degree sequence.

Our experiments do not contradict the general ideas about robustness commonly held since Albert et al. [2], but indicate that differences between scale-free and uniform random graphs are exaggerated by preferential attachment.

Using two newly introduced variants of the Havel-Hakimi algorithm, it was even possible to construct scale-free graphs that are indistinguishable in terms of their degree sequence (and thus scale-freeness) but either extremely fragile or not fragile at all. Statements about the robustness of scale-free networks should therefore be interpreted as stylized rather than absolute.

More generally, one should be hesitant to draw conclusions about scale-free networks from computational experiments in which all instances are generated from preferential attachment.

References

[1] G. W. Klau and R. Weiskircher, "Robustness and resilience," in *Network Analysis*, ser. Lecture Notes in Computer Science (LNCS), U. Brandes and T. Erlebach, Eds. Springer-Verlag, 2005, vol. 3418, pp. 417–437.

[2] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[3] J. C. Doyle, D. L. Alderson, L. Li, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, "The 'robust yet fragile' nature of the Internet," *Proceedings of the National Academy of Sciences (PNAS)*, vol. 102, no. 41, pp. 14 497–14 502, 2005.

[4] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[5] C. Petersen, N. Rotbart, J. G. Simonsen, and C. Wulff-Nilsen, "Near optimal adjacency labeling schemes for power-law graphs," in *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[6] L. Li, D. Alderson, J. C. Doyle, and W. Willinger, "Towards a theory of scale-free graphs: Definition, properties, and implications," *Internet Mathematics*, vol. 2, no. 4, pp. 431–523, 2005.

[7] M. E. J. Newman, "Assortative mixing in networks," *Phys. Rev. Lett.*, vol. 89, p. 208701, Oct 2002.

[8] I. Gutman and N. Trinajstić, "Graph theory and molecular orbitals. total π-electron energy of alternant hydrocarbons," *Chemical Physics Letters*, vol. 17, pp. 535–538, 1972.

[9] P. Erdös and A. Rényi, "On random graphs I," *Publicationes Mathematicae Debrecen*, vol. 6, pp. 290–297, 1959.

[10] V. Havel, "Poznámka o existenci konečnỳch grafů (Czech) [A remark on the existence of finite graphs]," *Časopis pro pěstování matematiky*, vol. 080, no. 4, pp. 477–480, 1955.

[11] S. L. Hakimi, "On realizability of a set of integers as degrees of the vertices of a linear graph. I," *Journal of the Society for Industrial and Applied Mathematics*, vol. 10, no. 3, pp. 496–506, 1962.

[12] D. L. Wang and D. J. Kleitman, "On the existence of n-connected graphs with prescribed degrees ($n \geq 2$)," *Networks*, vol. 3, no. 3, pp. 225–239, 1973.

[13] B. Bollobás, O. Riordan, J. Spencer, and G. Tusnády, "The degree sequence of a scale-free random graph process," *Random Structures and Algorithms*, vol. 18, pp. 279–290, 2001.

[14] S. N. Dorogovtsev, J. F. F. Mendes, and A. N. Samukhin, "Structure of growing networks with preferential linking," *Phys. Rev. Lett.*, vol. 85, pp. 4633–4636, Nov 2000.

[15] C. M. Schneider, A. A. Moreira, J. S. Andrade Jr, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences (PNAS)*, vol. 108, no. 10, pp. 3838–3841, 2011.

[16] T. Asano, "An $\mathcal{O}(n \log \log n)$ time algorithm for constructing a graph of maximum connectivity with prescribed degrees," *Journal of Computer and System Sciences*, vol. 51, no. 3, pp. 503–510, 1995.

[17] H. Kim, Z. Toroczkai, P. L. Erdős, I. Miklós, and L. A. Székely, "Degree-based graph construction," *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 39, p. 392001, 2009.

[18] P. Erdös, "On the evolution of random graphs," *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[19] A. Clauset, C. R. Shalizi, and M. E. Newman, "Power-law distributions in empirical data," *SIAM review*, vol. 51, no. 4, pp. 661–703, 2009.

[20] G. Csardi and T. Nepusz, "The igraph software package for complex network research," *InterJournal*, vol. Complex Systems, p. 1695, 2006.
[21] F. Viger and M. Latapy, "Efficient and simple generation of random simple connected graphs with prescribed degree sequence," in *International Computing and Combinatorics Conference*. Springer, 2005, pp. 440–449.
[22] T. P. Peixoto, "The graph-tool python library," *figshare*, 2014.
[23] P. Virtanen, R. Gommers, T. E. Oliphant, M. Haberland, T. Reddy, D. Cournapeau, E. Burovski, P. Peterson, W. Weckesser, J. Bright *et al.*, "Scipy 1.0: fundamental algorithms for scientific computing in python," *Nature Methods*, pp. 1–12, 2020.
[24] R. Xulvi-Brunet and I. M. Sokolov, "Reshuffling scale-free networks: From random to assortative," *Phys. Rev. E*, vol. 70, p. 066102, Dec 2004.
[25] U. Brandes and T. Erlebach, Eds., *Network Analysis*, ser. Lecture Notes in Computer Science (LNCS). Springer-Verlag, 2005, vol. 3418.
[26] A. R. Rao and S. B. Rao, "On factorable degree sequences," *Journal of Combinatorial Theory B*, vol. 13, pp. 185–191, 1972.
[27] V. Chungphaisan, "Construction of Hamiltonian graphs and bigraphs with prescribed degrees," *Journal of Combinatorial Theory B*, vol. 24, no. 2, pp. 154–163, 1978.
[28] B. Bollobás, *Extremal graph theory*. Courier Corporation, 2004.
[29] T. M. Apostol, *Introduction to analytic number theory*. Springer Science & Business Media, 2013.
[30] J. Havil, *Gamma: Exploring Euler's Constant*. Princeton University Press, 2010, vol. 84.

APPENDIX

A. Realizability of H^3

With the following results from the literature, we can split the proof of Theorem 2 into two smaller parts.

Lemma 1: [26] [27] A graphical sequence $D = (d_1, \dots, d_n)$ can be realized with a Hamiltonian cycle, if and only if $(d_1 - 2, \dots, d_n - 2)$ is graphical and

$$\frac{1}{k}\sum_{i=1}^{k}(d_i - d_{n-i+1}) < n - k - 1$$

for all $k \in \{1, \dots, \lceil \frac{n}{2} \rceil - 1\}$. Furthermore, If D can be realized with a Hamiltonian cycle, then it can also be realized with a Hamiltonian cycle in which the vertices appear in order of their degrees.

The first part is to show that a scaling degree sequence remains graphical after reducing all degrees by two when planting the Hamiltonian cycle. This is proven in the next section.

Lemma 2: Let $D = (d_1, d_2, \dots, d_n)$ be a scaling degree sequence with $\gamma > 1$ and $d_n \geq 2$. For sufficiently large n, $(d_1 - 2, \dots, d_n - 2)$ is graphical.

The second part consists of bounds on the differences between high and low degrees.

Lemma 3: Let $D = (d_1, d_2, \dots, d_n)$ be a scaling integer sequence with $\gamma > 1$ and $d_n \geq 2$. For sufficiently large n,

$$\frac{1}{k}\sum_{i=1}^{k}(d_i - d_{n-i+1}) < n - k - 1$$

for all $k \in \{1, \dots, \lceil \frac{n}{2} \rceil - 1\}$.

Proof: Notice that $d_i = n^{\frac{1}{\gamma}} d_n i^{-\frac{1}{\gamma}}$. Fix any $k \in \{1, \dots, \lceil \frac{n}{2} \rceil - 1\}$. Then, again exploiting the scaling property,

$$\frac{1}{k}\sum_{i=1}^{k}(d_i - d_{n-i+1}) = \frac{n^{\frac{1}{\gamma}} d_n}{k}\sum_{i=1}^{k}\underbrace{\left[i^{-\frac{1}{\gamma}} - (n-i+1)^{-\frac{1}{\gamma}}\right]}_{\leq 1}$$
$$\leq n^{1/\gamma} d_n \in o(n),$$

and therefore less than $n - k - 1$ for n sufficiently large. ∎

B. Proof of Lemma 2

We use the following condition to show that the residual sequence is graphical.

Lemma 4: [28] An integer sequence $d_1, d_2, \dots, d_n$ with $n > d_1 \geq d_2 \geq \cdots \geq d_n$ is graphical if and only if $\sum_{i=1}^{n} d_i$ is even and for all $t \in \{1, \dots, n\}$:

$$2\sum_{i=1}^{t} d_i \leq \sum_{i=1}^{n} d_i + \sum_{i=1}^{t} \min\{d_i, t-1\}.$$

To bound the terms in these conditions, we use the following approximation.

Lemma 5: [29] Let $\zeta(z)$ be the Euler's generalized constant defined for $z \in (0, 1)$ [30]. For $t \geq 1$ and $\gamma > 1$:

$$\sum_{i=1}^{t} i^{-\frac{1}{\gamma}} = \frac{t^{1-\frac{1}{\gamma}}}{1-\frac{1}{\gamma}} + \zeta(\frac{1}{\gamma}) + O(t^{-\frac{1}{\gamma}}).$$

Lemma 6: If $d_1, \dots, d_n$ is a scaling integer sequence with $\gamma > 1$, $\sum_{i=1}^{d_1} d_i \in o(n)$ and $\sum_{i=1}^{n}(d_i - 2) \in \Omega(n)$.

Proof: Notice that $d_i = n^{\frac{1}{\gamma}} d_n i^{-\frac{1}{\gamma}} = d_1 i^{-\frac{1}{\gamma}}$ and $\gamma^2 > 2\gamma - 1 > 1$. Using Lemma 5 we obtain

$$\sum_{i=1}^{d_1} d_i = d_1 \sum_{i=1}^{d_1} i^{-\frac{1}{\gamma}} \in \Theta(d_1^{2-\frac{1}{\gamma}}) = \Theta(n^{\frac{2\gamma-1}{\gamma^2}} d_n^{\frac{2\gamma-1}{\gamma}}) \in o(n)$$

as well as

$$\sum_{i=1}^{n}(d_i - 2) = n^{\frac{1}{\gamma}} d_n \sum_{i=1}^{n} i^{-\frac{1}{\gamma}} - \underbrace{2n}_{\leq n d_n}$$
$$\geq n^{\frac{1}{\gamma}} d_n \left(\frac{n^{1-\frac{1}{\gamma}}}{1-\frac{1}{\gamma}} + o(n^{1-\frac{1}{\gamma}})\right) - n d_n$$
$$= n\left(\frac{1}{\gamma - 1} d_n\right) + o(n) \ \in \ \Omega(n) \ . \qquad \blacksquare$$

We can now show that the conditions required in Lemma 4 hold. Notice that $\sum_{i=1}^{n}(d_i - 2) = \sum_{i=1}^{n} d_i - 2n$ is even since $\sum_{i=1}^{n} d_i$ is even. We only need to prove $\forall t \in \{1, \dots, n\}$: $\sum_{i=1}^{n}(d_i - 2) - 2\sum_{i=1}^{t}(d_i - 2) + \sum_{i=1}^{t} \min\{d_i - 2, t-1\} \geq 0$. If $t \geq d_1 - 1$ the statement is equivalent to $\sum_{i=t+1}^{n}(d_i - 2) \geq 0$ which trivially holds. In case $t \leq d_1 - 2$, we use Lemma 6 to complete the proof of Lemma 2 by

$$\underbrace{\sum_{i=1}^{n}(d_i - 2)}_{\in \Omega(n)} - 2 \underbrace{\sum_{i=1}^{t}(d_i - 2)}_{< \sum_{i=1}^{d_1} d_i \in o(n)} + \underbrace{\sum_{i=1}^{t} \min\{d_i - 2, t-1\}}_{\geq 0} \in \Omega(n) \ .$$