Postprint: Robustness Study of Topology-Tunable Scale-Free Networks Under Cost Considerations

Authors: Wang Ershen, Wang Yuwei

Date: 2018-05-20T00:00:00+00:00

Abstract

To investigate the influence of scale-free network topology on network robustness, we propose a cost-aware attack method for topology-adjustable scale-free networks by incorporating two critical metrics affecting complex network robustness: node betweenness and edge weight. This method introduces attack cost factors for nodes (edges) during network attacks, approximating the attack cost of nodes (edges) using node betweenness (edge weight). Various node (edge) attack strategies are employed to attack the network, with the relative size of the largest connected component adopted as the network robustness metric. Using this method, we systematically study the relationships between the power-law exponent, average degree, and network robustness in scale-free networks. The results demonstrate that under deliberate attack strategies, for a given node (edge) attack cost, scale-free networks exhibit stronger robustness when the power-law exponent is smaller or the average degree is larger. Simulation experiments validate the effectiveness and feasibility of the proposed method.

Full Text

Research on Robustness of Tunable Scale-Free Networks with Cost Considerations

Wang Ershena,b, **Wang Yuwei**a
aSchool of Electronic & Information Engineering, bLiaoning General Aviation Key Laboratory, Shenyang Aerospace University, Shenyang 110136, China

Abstract

To investigate the influence of scale-free network topology on network robustness, this paper proposes a tunable scale-free network attack method that incor-

porates cost considerations by combining two key metrics—node betweenness and edge weight—that significantly impact network robustness. The method introduces attack cost factors for nodes (edges) during network attacks, using node betweenness (edge weight) to approximate the attack cost of nodes (edges). Different node (edge) attack strategies are employed, and the relative size of the largest connected component is adopted as the network robustness metric. Using this method, we examine the relationship between the power-law exponent, average degree, and robustness of scale-free networks. The results demonstrate that under intentional attack strategies with fixed node (edge) attack costs, scale-free networks with smaller power-law exponents or larger average degrees exhibit stronger robustness. Simulation experiments validate the effectiveness and feasibility of the proposed method.

Keywords: scale-free networks; power-law exponent; average degree; attack strategy; attack cost; robustness

0 Introduction

In recent years, complex networks have attracted increasing attention from scholars. As research on complex networks has deepened, their robustness has become a hot topic. Complex network robustness refers to the ability of a network to maintain its functionality when subjected to attacks. Significant progress has been made in complex network robustness research. For instance, reference [4] used natural connectivity as a robustness metric to study the impact of degree distribution, concluding that more non-uniform degree distributions yield stronger robustness. Reference [5] analyzed the robustness of vehicular ad-hoc networks, finding them robust against random attacks but vulnerable to intentional attacks. However, these studies did not incorporate attack cost factors for nodes (edges).

Reference [12] recognized this limitation and attempted to consider node attack costs in robustness analysis by using node degree to approximate attack cost. Their findings indicated that when attack costs are small, the low-degree removal strategy (LDRS) is most effective, while the high-degree removal strategy (HDRS) is only optimal when attack costs are large, demonstrating that attack costs influence the effectiveness of attack strategies. However, these studies did not use node betweenness to measure attack costs, nor did they consider edge attack costs when attacking network edges.

Building upon previous research, this paper first introduces a cost-based tunable scale-free network attack model, then investigates how the power-law exponent and average degree affect the robustness of scale-free networks, and finally presents the main conclusions.

1 Model and Methods

1.1 Tunable Scale-Free Networks

The BA (Barabasi-Albert) scale-free network has a fixed power-law exponent of 3, whereas many real-world complex networks with scale-free characteristics have exponents between 2 and 3. A smaller exponent γ indicates stronger non-uniformity in the degree distribution, while a larger γ indicates greater uniformity. Reference [1] proposed an algorithm for generating scale-free networks with adjustable power-law exponents.

1.2 Betweenness

Betweenness is divided into node betweenness and edge betweenness, reflecting the influence of nodes (edges) in the network. Node betweenness is defined as:

$$B_i = \sum_{j \neq l \neq i} \frac{\delta_{jl}(i)}{\delta_{jl}}$$

where δ_{jl} is the number of shortest paths between nodes j and l, and $\delta_{jl}(i)$ is the number of those shortest paths that pass through node i.

1.3 Weighted Complex Networks

Many real-world networks are weighted networks. For example, different links in the Internet have varying bandwidth and traffic, and airline networks exhibit differences in passenger flow. Such information cannot be described using unweighted networks, necessitating weighted networks where each edge is assigned a weight to reflect these differences. A weighted network can be described by the set $G(N, W)$, where N is the number of nodes and W represents edge weights, typically expressed as a weighted adjacency matrix $W = (w_{ij})_{n \times n}$.

Edge weights are related to the degrees of the two connected nodes. Assuming the degrees of nodes connected by edge e_{ij} are k_i and k_j, reference [10] defines the weight model as:

$$w_{ij} = (k_i k_j)^{\theta}$$

where θ is a tunable weight parameter describing the heterogeneity of network edges.

Reference [11] presents three weighting methods for complex network edges: $w_{ij} = B_{ij}$ (edge betweenness), $w_{ij} = (B_i B_j)^{\theta}$ (power-law form of the product of endpoint betweenness), and $w_{ij} = (k_i k_j)^{\theta}$ (power-law form of the product of endpoint degrees).

Combining these weighting approaches with node degree and node betweenness, this paper adopts a composite edge weighting method defined as:

$$w_{ij} = \frac{\alpha \max\{k_i, k_j\} + (1-\alpha)\max\{B_i, B_j\}}{\max\{k_i, k_j\} + \max\{B_i, B_j\}}$$

where α is a weighting coefficient. $\alpha = 0$ indicates edge weight is related only to node betweenness, while $\alpha = 1$ indicates edge weight is related only to node degree. This weighting approach in equation (3) allows flexible adjustment of the relative importance of betweenness and degree through parameter α. The edge weight comprehensively considers both node degree and node betweenness, and in this paper, α is set to 0.5.

1.4 Complex Network Robustness Metric

A network is considered robust to node (edge) failures if most nodes remain connected after removing a small fraction of nodes (edges). Various metrics exist for measuring complex network robustness, such as the largest connected component and average inverse geodesic distance. This paper uses the relative size of the largest connected component $G = N'/N$ to measure complex network robustness, where N' is the number of nodes in the largest connected component after attack and N is the total number of nodes before attack. Under a given attack strategy, a larger G value indicates stronger network robustness and less effective attack.

1.5 Attack Strategies

1.5.1 Node Attack Strategies Reference [12] employs three node degree attack strategies: Low Degree Removal Strategy (LDRS), Random Degree Removal Strategy (RDRS), and High Degree Removal Strategy (HDRS).

Improving upon these degree-based probabilistic removal methods, we derive the following node removal approach based on node betweenness (when a node is removed, its connected edges also disappear):

- **Low Betweenness Removal Strategy (LBRS)**: Remove nodes sequentially in ascending order of their betweenness values.
- **Random Betweenness Removal Strategy (RBRS)**: Remove nodes randomly selected based on their betweenness values.
- **High Betweenness Removal Strategy (HBRS)**: Remove nodes sequentially in descending order of their betweenness values.

For the model parameter β, this paper selects three cases ($\beta = -3$, $\beta = 0$, and $\beta = 3$) to determine node betweenness attack strategies.

1.5.2 Edge Attack Strategies Edge attack strategies are defined based on edge weight and other importance metrics, where edges are sorted and removed according to their weights. This paper employs three edge attack strategies:

a) **Random Weight Removal Strategy (RWRS)**: Remove edges randomly selected based on edge weights.

b) **Low Weight Removal Strategy (LWRS)**: Remove edges sequentially in ascending order of edge weights.

c) **High Weight Removal Strategy (HWRS)**: Remove edges sequentially in descending order of edge weights.

1.6 Attack Cost

1.6.1 Node Betweenness Attack Cost Various metrics measure node importance in complex networks, including degree, betweenness, closeness, and eigenvector centrality. Reference [12] approaches attack cost from the "node degree" perspective, using node degree to approximate attack cost, with total node degree attack cost defined as:

$$\mu = \sum_{i \in Z} \frac{k_i}{\sum_{v \in N} k_v}$$

where k_i is the degree of node i, N is the total number of nodes in the initial network, Z is the set of removed nodes, and $\sum_{i \in Z} k_i$ is the sum of degrees of removed nodes.

Recognizing that node betweenness is also an important metric, this paper approaches attack cost from the "node betweenness" perspective, using node betweenness to approximate attack cost and assuming attack cost is proportional to node betweenness. Total node betweenness attack cost is defined as:

$$\rho = \sum_{i \in Z} \frac{B_i}{\sum_{v \in N} B_v}$$

where B_i is the betweenness of node i, N is the total number of nodes in the initial network, Z is the set of removed nodes, and $\sum_{i \in Z} B_i$ is the sum of betweenness values of removed nodes.

1.6.2 Edge Attack Cost Previous studies often ignore edge attack cost factors, yet edge attack costs in complex networks may not be uniform. To study how edge attack costs affect various edge attack strategies, this paper uses edge weight to measure attack cost, with total edge attack cost defined as:

$$\lambda = \sum_{i \in M} \frac{w_i}{\sum_{e \in L} w_e}$$

where w_i is the weight of edge i, L is the set of all edges in the network, M is the set of removed edges, and $\sum_{i \in M} w_i$ is the sum of weights of removed edges.

1.7 Algorithm Flow

Based on the definitions in Sections 1.1–1.6, the algorithm for the complex network node (edge) attack model based on betweenness (edge) cost is designed as follows:

a) Generate a scale-free network of a certain size with adjustable exponent using the algorithm in Section 1.1.

b) Calculate the betweenness of each node using equation (1); for edge attacks, calculate the weight of edges between nodes using equation (3).

c) Remove network nodes according to the probability in equation (4); for edge attacks, attack complex network edges using the edge attack strategies in Section 1.5.2.

d) Set the initial cost value for complex network nodes, and recalculate the ρ value using equation (6) for the removed nodes' betweenness. If the ρ value is smaller than the given cost value, remove this node and repeat steps (c)-(d) until the ρ value reaches the given node cost value. For edge attacks, set the initial cost value for complex network edges, calculate the λ value using equation (7) for attacked edges, and if the λ value is smaller than the given cost value, remove the edge and repeat until the λ value reaches the given edge cost value.

e) Calculate the relative size of the largest connected component G.

2 Simulation Verification and Analysis

This section investigates the effects of power-law exponent and average degree on the robustness of tunable scale-free networks when cost factors are considered. Each experiment is conducted independently 40 times, with final results obtained by averaging.

2.1 Effect of Power-Law Exponent on Robustness

To explore the impact of the power-law exponent on network robustness, we generate scale-free networks with $N = 1000$ nodes using the aforementioned tunable mechanism and test different exponent values.

The effects of power-law exponent on network robustness under node degree attack strategies are shown in [Figure 1: see original paper]. Under node betweenness attack strategies, the effects are shown in [Figure 2: see original paper]. Under edge attack strategies, the effects are shown in [Figure 3: see original paper].

[Figure 1: see original paper] shows the robustness curves for different node degree attack strategies. From Figure 1: see original paper, using LDRS, smaller γ values produce steeper robustness curves, indicating poorer network robustness. From Figure 1: see original paper, using RDRS, different γ values have almost identical effects on robustness. From Figure 1: see original paper, using HDRS, smaller γ values produce slower declining robustness curves, indicating stronger network robustness.

[Figure 2: see original paper] shows robustness curves for different node betweenness attack strategies. In Figure 2: see original paper using LBRS, smaller γ values yield poorer robustness. In Figure 2: see original paper using RBRS, $\gamma = 2.2$ shows a larger variation trend than other γ values, but the overall trend is similar. In Figure 2: see original paper using HBRS, smaller γ values correspond to stronger robustness.

[Figure 3: see original paper] shows robustness curves for different edge attack strategies. In Figure 3: see original paper using LWRS, when $\lambda < 0.3$, smaller γ yields poorer robustness; when $0.31 < \lambda < 0.55$, larger γ yields weaker robustness; and when $\lambda > 0.55$, the network robustness is weakest at $\gamma = 2.2$. Figure 3: see original paper uses RWRS: when $\lambda < 0.38$, larger γ yields stronger robustness; when $0.38 < \lambda < 1$, smaller γ yields stronger robustness; and when $\lambda > 1$, different γ values produce nearly identical robustness curves, indicating that under RWRS with large attack costs, γ has minimal impact. Figure 3: see original paper uses HWRS: smaller γ values correspond to stronger robustness.

2.2 Effect of Average Degree on Robustness

To study the effect of average degree on robustness of exponent-adjustable scale-free networks, we set the power-law exponent $\gamma = 3$ and vary the average degree $\langle k \rangle$ of the scale-free network.

The effects under node degree attack strategies are shown in [Figure 4: see original paper], under node betweenness attack strategies in [Figure 5: see original paper], and under edge attack strategies in [Figure 6: see original paper].

[Figure 4: see original paper] shows robustness curves for node degree attack strategies. In Figure 4: see original paper using LDRS, curves for different average degrees nearly coincide, indicating minimal impact of average degree on robustness. In Figure 4: see original paper using RDRS, when $\mu < 0.5$, smaller average degree yields weaker robustness; when $\mu > 0.5$, different average degrees have almost identical effects. In Figure 4: see original paper using HDRS, when $\mu < 0.5$, larger average degree yields stronger robustness; when $\mu > 0.5$, different average degrees have almost identical effects.

[Figure 5: see original paper] shows robustness curves for node betweenness attack strategies. In Figure 5: see original paper using LBRS, smaller average degree yields stronger robustness. In Figure 5: see original paper using RBRS, smaller average degree yields weaker robustness. In Figure 5: see original paper using HBRS, larger average degree yields stronger robustness.

[Figure 6: see original paper] shows robustness curves for edge attack strategies. In Figure 6: see original paper using LWRS, larger average degree yields stronger robustness. In Figure 6: see original paper using RWRS, when $\lambda < 0.5$, larger average degree yields stronger robustness; when $\lambda > 0.5$, different average degrees have almost identical effects. In Figure 6: see original paper using HWRS, smaller average degree yields weaker robustness.

3 Conclusion

Based on previous complex network robustness research, this paper incorporates node and edge attack cost factors to investigate how power-law exponent and average degree affect the robustness of tunable scale-free networks. The study reveals that when attack costs are non-negligible and intentional attack strategies are employed (such as HDRS, HBRS, or HWRS), scale-free networks with smaller power-law exponents (more heterogeneous degree distributions) or larger average degrees (denser networks) exhibit stronger robustness and are more difficult to disrupt.

References

[1] Goh K I, Kahng B, Kim D. Universal behavior of load distribution in scale-free networks [J]. Physical Review Letters, 2001, 87 (27): 278701.
[2] Hong Chen, He Ning, Lordan O, et al. Efficient calculation of the robustness measure R for complex networks [J]. Physica A: Statistical Mechanics and its Applications, 2017, 478: 63-68.
[3] Nie Tingyuan, Guo Zheng, Zhao Kun, et al. New attack strategies for complex networks [J]. Physica A: Statistical Mechanics and its Applications, 2015, 424: 248-253.
[4] 吴俊, 谭索怡, 谭跃进, 等. 基于自然连通度的复杂网络鲁棒性分析 [J]. 复杂系统与复杂性科学, 2014, 11 (1): 77-86.
[5] 冯慧芳, 李彩虹. 基于复杂网络的车载自组织网络鲁棒性分析 [J]. 计算机应用, 2016, 36 (7): 1789-1792, 1806.
[6] 陆靖桥, 傅秀芬, 蒙在桥. 复杂网络的鲁棒性与中心性指标的研究 [J]. 计算机应用与软件, 2016, 33 (4): 302-309.
[7] 谢逢洁, 崔文田. 加权快递网络鲁棒性分析及优化 [J]. 系统工程理论与实践, 2016, 36 (9): 2391-2399.
[8] Motter A E, Lai Y C. Cascade-based attacks on complex networks [J]. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2002, 66 (6): 065102.
[9] 彭兴钊, 姚宏, 张志浩, 等. 基于节点蓄意攻击的无标度网络级联抗毁性研究 [J]. 系统工程与电子技术, 2013, 35 (9): 1974-1978.
[10] Wang Wenxu, Chen Guanrong. Universal robustness characteristic of weighted networks against cascading failure [J]. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2008, 77 (2): 026101.
[11] Mirzasoleiman B, Babaei M, Jalili M, et al. Cascaded failures in weighted networks [J]. Physical Review E: Statistical Nonlinear and Soft Matter Physics, 2011, 84 (2): 046114.
[12] Hong Chen, Cao Xianbin, Du Wenbo, et al. The effect of attack cost on network robustness [J]. Physica Scripta, 2013, 87 (5): 458-465.

Note: Figure translations are in progress. See original paper for figures.