Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/6/20230748

Network resilience: impact on small-world network

Chuanshi Wang

School of Information Science and Engineering, Lanzhou University, Lanzhou, 730000, PR China

wangchsh20@lzu.edu.cn

Abstract. Lots of complex systems in the real world have network structures, and a number of these structures have small-world property. This kind of structures are called small-world networks. Examples include the world's air transportation system, electric power systems, and human functional brain network, and small-world property is one of the key reasons why these systems function efficiently. However, for complex systems, in addition to their efficiency, resilience or robustness is also one of the concerns, as these systems need to ensure that they do not completely collapse on their own in case of failure of a small number of their components. The purpose of this paper is to try to find and explain the factors that affect the robustness of small-world network by comparing different classes of small-world networks and analysing differences between them and possible causes of these differences, in order to get an idea to optimize the robustness of small-world networks while preserving their small-world property.

Keywords: small-world network, robustness, broad-scale network, single-scale network.

1. Introduction

Network structure is a very common complex structure in real world, and this structure has many good properties. The study on network structure helps humans to better understand and use concrete or abstract things with such structures. One of the quite noteworthy properties is small-world property.

Small-world property is not universal, for example, regular lattice does not have small-world property. However, for networks with small-world property, the expectation of the distance between any two nodes in the network grows in the same order as the logarithm of the network size, provided that the degree distribution of nodes is determined [1, 2]. For networks with small-world property, even if a lot of nodes are contained, the communication between any two points often requires few nodes to be established.

Because of the aging of vertices and the limited capacity of vertices, behaviors such as preferential attachment tend to be suppressed to varying degrees during the growth of real networks, and thus the scale-free degree distribution is affected to different degrees [3]. Among the networks that can eventually maintain small-world property, they can be classified into the following three types based on the degree distribution: scale-free networks, broad-scale networks and single-scale networks [3].

By using the Molloy-Reed Criterion, the criterion for criticality for the disruption of a network's giant component can be obtained by the following equation [4]:

DOI: 10.54254/2755-2721/6/20230748

$$f_c = 1 - \frac{1}{\frac{\langle k^2 \rangle}{\langle k \rangle} - 1} \tag{1}$$

This indicates that the resilience of the network is related to the first-order moment and second-order moment of all nodes' degree, which means the resilience of network is related to degree distribution. Therefore, even if they are the same small-world networks, their resilience can differ. This paper aims to investigate the differences in resilience among different small-world networks caused by various degree distributions, and discuss some possibility of preserving the small-world property while making networks highly robust.

2. Classes of small-world networks

2.1. Scale-free networks

In such class of networks, degree of nodes decays with the power law. The following equation is about scale-free networks' degree distribution [3, 5]:

$$p_k = Ck^{-\gamma} \tag{2}$$

Because of power-law distribution itself and peculiarities of the degree exponent, the first- and second-order moments of the degree of such networks are in most cases divergent and there is no meaningful scale [6], so such networks are called scale-free networks. When the degree exponent satisfies $2 < \gamma < 3$, such networks are called ultrasmall worlds, because the expectation of the distance between any two points in them is even lower than the logarithmic order of the network size, which can be expressed by the following equation [5]:

$$\langle d \rangle \sim \ln \ln N \tag{3}$$

The ultra-small world network is extremely robust to random errors, ensuring connectivity between most of the remaining nodes even if the vast majority of them suffer failures. It is not robust against targeted attacks, as the removal of a tiny number of hub nodes is sufficient to severely disrupt the network topology [7].

It is clear that the number of low degree nodes is much greater than the number of high degree nodes in such networks because of power-law distribution, and therefore such networks always exhibit a decentralized topology with a lot of small nodes connected by several hub nodes.

2.2. Broad-scale networks

While network growing, the preferential attachment causes the degree distribution of nodes in the network to satisfy the power-law distribution in general [8], but in real world networks, because of constraints such as aging of vertices and limited capacity of vertices, behaviours such as preferential attachment in the process of network growth are suppressed to different degrees, resulting in exponential decay or Gaussian decay of the degree distribution in the tail [3].

Considering node aging in the process of simulating network evolution, i.e., letting nodes attract new links at a gradually decreasing rate with iteration, will make the final generated network have a weaker power-law mechanism than the original BA model, i.e., let the network tend to be homogeneous; when the aging effect of the simulation is strong enough, the network will completely lose its scale-free property [3, 9].

A similar effect is produced by considering the capacity limit of nodes during network growth, i.e., nodes whose degree reaches a certain limit are not allowed to continue building new links during network growth [3].

2.3. Single-scale networks

The degree distribution of such networks has a rapidly decaying tail and usually obeys a probability distribution such as a Gaussian or exponential distribution [3]. In this class of networks, the scales of

DOI: 10.54254/2755-2721/6/20230748

such networks are meaningful because the first-order moment and second-order moment of degree do not diverge.

Random network has degree distribution obeying the binomial distribution, so there exists a single scale for such networks, which belong to single-scale networks. For a large random network, Poisson distribution is accurate enough to approximate its degree distribution with less variables, and the second-order moments of degree can be obtained from the Poisson distribution as:

$$\langle k^2 \rangle = \langle k \rangle (\langle k \rangle + 1) \tag{4}$$

From equation (1) and equation (4), the criterion for criticality of the random network can be obtained as follows:

$$f_c^{ER} = 1 - \frac{1}{\langle k \rangle} \tag{5}$$

For random networks, when the ratio of removed nodes to all nodes is higher than f_c^{ER}, the network will crack, that is, there will leave no giant component whose size increases with a same order as the whole original network [4]. From equation (5), it is clear that the expectation of degree determines the sensitivity of a random network to random errors, so the criterion for criticality needs to be raised by adding many links in the network.

In fact, random networks are not the only ones with such a property. Unlike scale-free networks, most nodes have degree fluctuating around ⟨k⟩ in single-scale networks because those networks own meaningful scale. The network always decomposes after randomly removing a certain percentage of nodes because it lacks robustness in case of random errors due to the absence of hub nodes.

3. Small-world network in real world

There is no standard scale-free network in reality, because the formation of a network with power-law degree distribution needs that the network has linear preferential attachment during growth, and the presence of facilitation or inhibition phenomena is not allowed [10], which is difficult to guarantee in reality. Therefore, the study of such small-world networks is often limited to the analysis of theoretical models such as the BA model or the ideal approximation of the real network structure, while few real network structures directly correspond to them.

When discussing real world scale-free networks, it always actually tends to discuss networks with a broad-scale or truncated scale-free degree distribution, i.e., scale-free networks with truncation. Movie actor network, the Internet, and human functional brain network belong to such small-world networks [3, 4, 11].

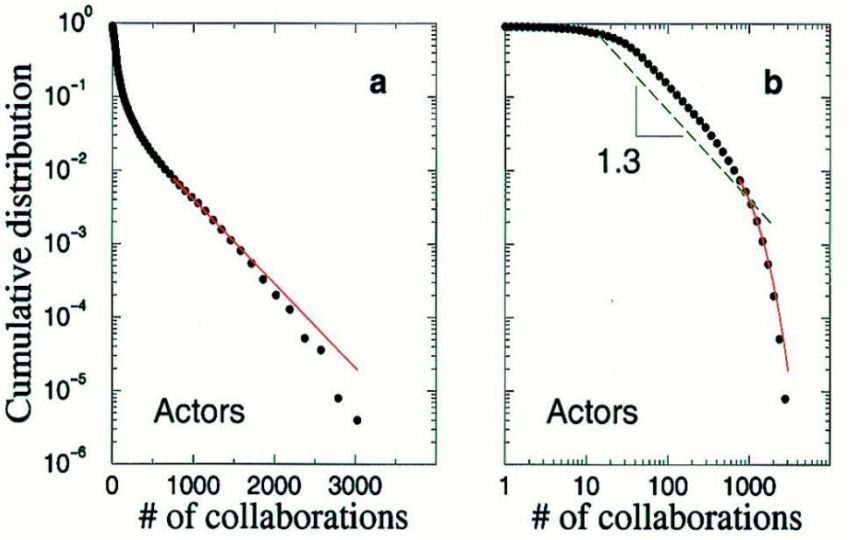

Figure 1. Network of movie actors [3].

DOI: 10.54254/2755-2721/6/20230748

Taking the movie actor network as an example, in figure 1 there is a real-world scale-free network, with low-degree saturation and high-degree truncation because of the presence of other constraints in the real world. The frequency of the low degree nodes is less than the predicted value of the power-law distribution due to low-degree saturation. The middle part of the degree distribution is better fitted by power-law distribution, and then there is a sharp decay in the tail, in this case exponential decay. Thus, the number of both low degree nodes and high degree nodes of the broad-scale network is significantly less than that of the scale-free network, which will make their properties exhibit differences.

Electric power grid and world airport network are real-world examples of single-scale networks [3], as presented in figure 2. In such small-world networks, the degrees of most nodes are similar to the first-order moment of degree because of the existence of scale, and the differences between nodes are not disparate. The network exhibits a decentralized pattern from which some of the properties in random networks originate, and thus it can be generalized to other single-scale networks as well.

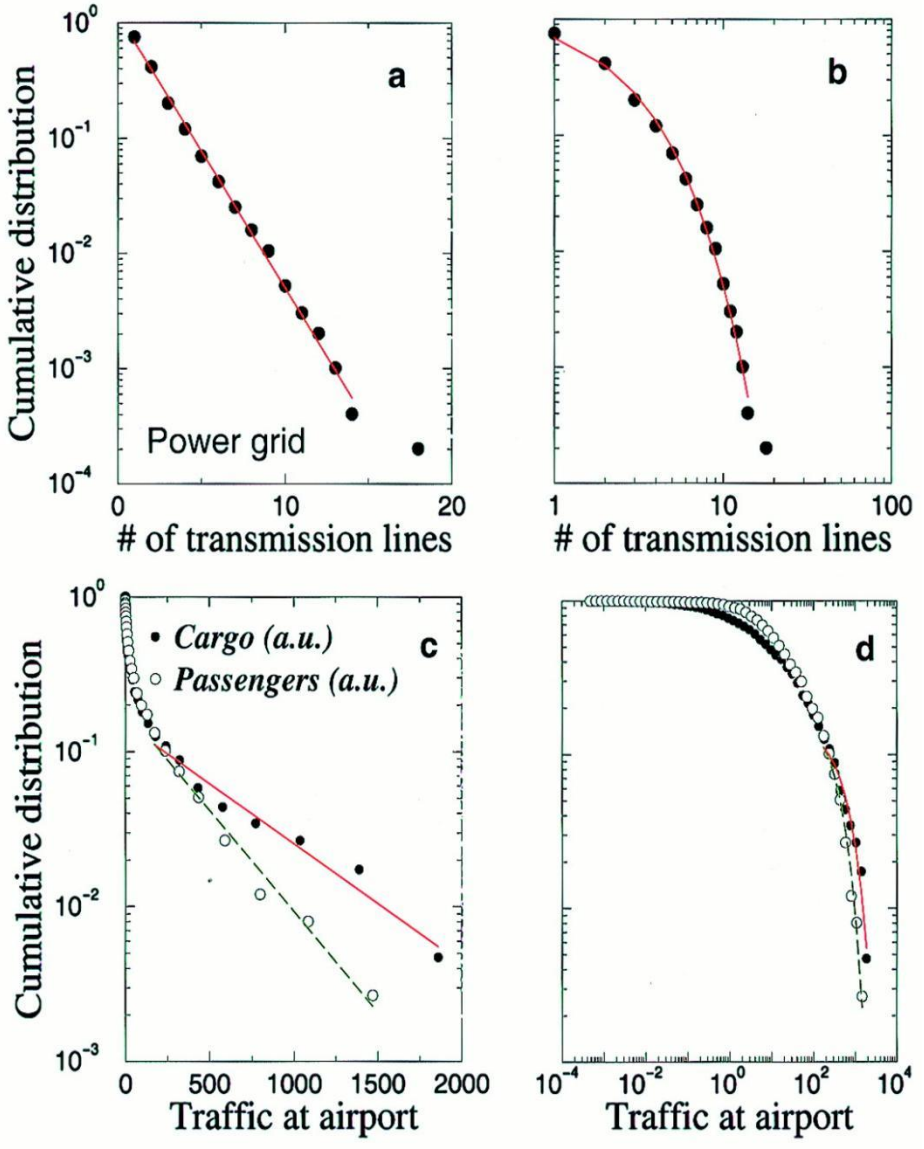

Figure 2. Electric power grid and the world airport network [3].

DOI: 10.54254/2755-2721/6/20230748

For dynamically growing networks, the network will completely lose its scale-free property and produce a degree distribution close to a Gaussian or exponential distribution when aging or capacity constraints affect the preferential attachment of nodes sufficiently during the growth process [3, 9]. It is therefore possible that such networks arise due to the high cost of linking to new nodes to existing nodes in the real world or other constraints.

4. Impact on small-world networks

For scale-free networks, when $2 < \gamma < 3$, i.e., the network is an ultrasmall world. When the network size N is unlimited, there is $f_c \to 1$. That is, for a sufficiently large scale-free network, by randomly removing the nodes in it, all of nodes need to be removed to ensure that the remaining nodes cannot form a giant component, which explains that the scale-free network has excellent robustness to random errors. When $\gamma > 3$, the criterion for criticality f_c is only determined by the degree exponent γ as well as the minimum degree k_{min}, which means that for a given degree distribution, a scale-free network with $\gamma > 3$ will always be decomposed after removing a certain percentage of nodes. The remaining nodes will not be able to form a giant component [12]. In terms of robustness only, scale-free networks with $\gamma > 3$ exhibit properties consistent with random networks.

Facing to targeted attacks, criterion for criticality of scale-free network can be described by the following relation [13]:

$$f_c^{\frac{2-\gamma}{1-\gamma}} = 2 + \frac{2-\gamma}{3-\gamma} K_{min} \left(f_c^{\frac{3-\gamma}{1-\gamma}} - 1 \right) \tag{6}$$

From equation (6), it can be seen that the criterion for criticality of the scale-free network does not diverge with increasing network size in the face of targeted attacks. When γ is small, the critical threshold will also take a relatively small value, illustrating the vulnerability of the ultra-small-world network with $2 < \gamma < 3$ in the face of targeted attacks. When γ is large, the network can be approximated as a random network, exhibiting a similar robustness to that in the face of random errors. Therefore, as far as the robustness of the network is concerned, a scale-free network with $\gamma > 3$ can be considered equivalent to a random network.

As stated in 2.2, the Internet is a broad-scale network. The Internet is highly robust in the face of random errors of nodes. Even if close to 100% of them are randomly removed, the remaining nodes are guaranteed to have giant formed components [4]. Like scale-free networks, the Internet is highly sensitive to targeted attacks [13], which indicates that truncation of the distribution does not bring significant differences between the Internet and scale-free networks.

Human brain network also belongs to broad-scale networks. The degree distribution of nodes in human functional brain network satisfies power-law distribution with exponential truncation, which makes brain network not only robust to random errors, but also shows better resilience to targeted attacks similar to random networks. This property is due to the fact that human brain networks have fewer high-degree nodes and more medium-degree nodes compared to standard scale-free networks [11]. Therefore, for scale-free networks, imposing certain restrictions on the dominant role of hub nodes does not cause a significant decrease in the resilience of the network to random errors, but can effectively improve the resilience of the network in the face of targeted attacks.

Single-scaled networks, in the case of random networks, are always decomposed after removing a certain percentage of nodes, according to equation (1), because there is no divergence of criterion for criticality due to the existence of the network's scale. The robustness on targeted attacks and random errors and is similar for a random network. According to equation (5), the criterion for criticality of the random network is determined by the first-order moment of degree, and improving the network robustness requires adding a lot of new links to the network as a cost. Single-scale networks with different degree distributions show many differences in facing random errors and targeted attacks, for example, for networks with Gaussian-distributed degree distributions, the network is more sensitive to random errors when $\sigma^2 < \mu$ and to targeted attacks when $\sigma^2 > \mu$ [14].

DOI: 10.54254/2755-2721/6/20230748

5. Improved robustness

Here is a strategy to optimize the network robustness by designing degree distribution to make a better resilience on both random errors and targeted attacks: let only two types of nodes with degrees k_{min} and k_{max} exist in the network where the degree of only one node is k_{max} and the degrees of the rest of the nodes are k_{min}, thus forming a network with a degree distribution with a bimodal distribution [15]. This strategy can work because the probability that the failed node is the node with degree k_{max} is extremely low in the face of random failures because there is only one node with degree k_{max}; the remaining nodes can also maintain the connectivity of the network in the face of targeted attacks. This is also enlightening to recognize the differences in robustness between different kinds of small-world networks.

As was introduced, the formation of scale-free networks is greatly affected by the linear preferential attachment while growing. When the linear preferential attachment is suppressed, i.e., there is sublinear preferential attachment, the degree distribution of the network obeys an exponentially truncated power-law distribution, and a broad-scaled network is formed at this time. When the role of preferential attachment is very weak, the degree distribution obeys an exponential distribution and the network degenerates to a single-scaled network.

The robustness of the network can be quantified using the following equation [15]:

$$f_c^{tot} = f_c^{rand} + f_c^{targ} \tag{7}$$

That is, the robustness of a network can be expressed as the sum of the criterion for criticality of that network in the face of random errors and the criterion for criticality in the face of targeted attacks. The connectivity of scale-free networks is mainly maintained by a few high-degree nodes, and random errors are nearly impossible to affect these high-degree nodes, so there is a large f_c^{rand}, while targeted attacks are very easy to destroy high-degree nodes, so the f_c^{targ} is low; the nodes in single-scaled networks are relatively similar, and there is no significant difference caused by how the nodes are removed, so the f_c^{rand} is lower and the f_c^{targ} is higher than scale-free networks. By adding a certain degree of cost to the network growth phase, the network can be made more resilient to the targeted attacks at the cost of losing some of its scale-free property, ultimately generating a broad-scale network with a higher f_c^{tot}.

6. Conclusion

There are many kinds of networks with small-world property, and by classifying them and studying them separately, it is known that a major source of differences among small-world networks is the difference in preferential attachment and ultimately leads to different degree distributions and different robustness. By adding different degrees of cost to the process of adding new nodes to the network, the robustness of the final generated network can be adjusted.

Scale-free networks have excellent robustness on random errors severe weakness for targeted attacks. By increasing the cost of the network growth model with linear preference dependencies, the final generated network can be gradually approached from the original scale-free network to single-scale network with better robustness against targeted attacks, and the total robustness of the network shows a trend of increasing and then decreasing. By reasonably limiting the preferential attachment of the network appropriately, a network with better robustness against targeted attacks can be obtained at the cost of losing a portion of the scale-free property, and eventually a network with better robustness to both random errors and targeted attacks is obtained, which will be a small-world network where the degree distribution obeys an exponentially truncated power-law distribution.

References

[1] Van Leeuwen, J. (Ed.). (1991). Handbook of theoretical computer science (vol. A) algorithms and complexity. Mit Press.

[2] Bollobás, B. (1998). Random graphs. In Modern graph theory (pp. 215-252). Springer, New

DOI: 10.54254/2755-2721/6/20230748

York, NY.

[3] Amaral, L. A. N., Scala, A., Barthelemy, M., & Stanley, H. E. (2000). Classes of small-world networks. Proceedings of the national academy of sciences, 97(21), 11149-11152.

[4] Cohen, R., Erez, K., Ben-Avraham, D., & Havlin, S. (2000). Resilience of the internet to random breakdowns. Physical review letters, 85(21), 4626.

[5] Cohen, R., & Havlin, S. (2003). Scale-free networks are ultrasmall. Physical review letters, 90(5), 058701.

[6] Barabási, A. L., Albert, R., & Jeong, H. (1999). Mean-field theory for scale-free random networks. Physica A: Statistical Mechanics and its Applications, 272(1-2), 173-187.

[7] Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. nature, 406(6794), 378-382.

[8] Barabási, A. L., & Albert, R. (1999). Emergence of scaling in random networks. science, 286(5439), 509-512.

[9] Dorogovtsev, S. N., & Mendes, J. F. F. (2000). Evolution of networks with aging of sites. Physical Review E, 62(2), 1842.

[10] Jeong, H., Néda, Z., & Barabási, A. L. (2003). Measuring preferential attachment in evolving networks. EPL (Europhysics Letters), 61(4), 567.

[11] Joyce, K. E., Hayasaka, S., &Laurienti, P. J. (2013). The human functional brain network demonstrates structural and dynamical resilience to targeted attack. PLoS computational biology, 9(1), e1002885.

[12] Barabási, A. L. (2013). Network science. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 371(1987), 20120375.

[13] Cohen, R., Erez, K., Ben-Avraham, D., & Havlin, S. (2001). Breakdown of the internet under intentional attack. Physical review letters, 86(16), 3682.

[14] Yuan, X., Shao, S., Stanley, H. E., & Havlin, S. (2015). How breadth of degree distribution influences network robustness: comparing localized and random attacks. Physical Review E, 92(3), 032122.

[15] Paul, G., Tanizawa, T., Havlin, S., & Stanley, H. E. (2004). Optimization of robustness of complex networks. The European Physical Journal B, 38(2), 187-191.