Applied Network Science

RESEARCH Open Access

Link-limited bypass rewiring for enhancing the robustness of complex networks

Masaki Chujyo[1*] and Fujio Toriumi[1]

*Correspondence:
mchujyo@g.ecc.u-tokyo.ac.jp

[1] School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 1138656, Japan

Abstract

Real-world networks often encounter disruptions that can have profound societal impacts. Therefore, enhancing network robustness against random failures and targeted attacks is crucial. Bypass rewiring, in which adjacent nodes are immediately reconnected following node removal, has been proposed as a promising method for enhancing network robustness. However, this method typically requires numerous bypass links and incurs significant costs. In this paper, we propose link-limited bypass rewiring, in which bypass links are reconnected stochastically. Additionally, we investigate the relationship between the number of bypass links and robustness improvement. Our findings, which are based on analytical and numerical results, reveal a tradeoff relationship between the number of added bypass links and robustness enhancement. Notably, preferentially reconnecting high-degree nodes was found to be effective for improving robustness. These insights can inform the design of resilient systems in real-world networks, offering strategies for enhancing robustness against node removal.

Keywords: Robustness, Targeted attack, Rewiring, Recovery

Introduction

In modern society, numerous real-world systems, including the internet, transportation systems, and power grids, are globally connected and represented as complex networks with many nodes and links (Albert and Barabási 2002; Dorogovtsev et al. 2008; Newman 2018). Such networks are exposed to disturbances caused by various internal and external factors, including random failures caused by human error and malfunctions, and intentional attacks such as terrorist attacks. Because many systems assume that all nodes are reachable, fragmentation degrades their functionality and can even lead to complete failure. Therefore, the construction of networks that are robust against random failures or targeted attacks has become a prominent issue in network science (Beygelzimer et al. 2005; Schneider et al. 2011; Louzada et al. 2013; Wu and Holme 2011; Chan and Akoglu 2016; Chujyo and Hayashi 2021).

Many real-world networks have a scale-free property that makes them vulnerable to degree-based targeted attacks. Scale-free networks have power-law degree distributions, which implies that a few hub nodes have many links. Because degree-based targeted attacks remove nodes with higher degrees, scale-free networks can be rapidly broken into smaller subnetworks (Albert et al. 2000). In contrast, scale-free networks are robust to random failures (random node removal). These findings have been analytically discussed as percolation transitions in scale-free networks (Cohen et al. 2000, 2001).

Previous studies have attempted to improve robustness against attacks by linking nodes with similar degrees (Schneider et al. 2011; Tanizawa et al. 2012; Wu and Holme 2011; Louzada et al. 2013; Hayashi 2018). Degree correlation represents the tendency of connection between similar nodes (Newman 2002). Networks with positive degree correlation are robust to random failures and targeted attacks (Newman 2002; Schneider et al. 2011). This is because in networks with positive degree correlation, nodes with lower degrees tend to be linked to each other, meaning connectivity is preserved even when attacks remove nodes with higher degrees. Degree correlation has also been analytically discussed as a type of percolation process (Goltsev et al. 2008; Tanizawa et al. 2012).

Bypass rewiring is an effective method for improving robustness against random failures or targeted attacks (Park and Hahn 2016; Park et al. 2019). In bypass rewiring, after a node is removed, the neighboring nodes are immediately re-linked. Bypass rewiring can achieve optimal robustness even if node pairs are selected randomly. Each neighboring node is selected and connected only once. Therefore, the degrees of nodes remain almost unchanged following node removal. Regarding its application in real-world networks, the main advantage of bypass rewiring is that there is no need to establish a new connection port at each node. For example, in an airline network, when an airport ceases to function, planes bypass that airport and head to surrounding airports to maintain transportation for the entire network. In reality, factors such as the number of flights in service will affect transportation. However, overall connectivity can be maintained while preventing increases in node degrees.

Although bypass rewiring is promising for improving robustness, research on its application to more realistic networks is still insufficient. Bypass rewiring requires many rewiring links, which increase costs. When applying bypass rewiring to large networks, the number of rewiring links is large and the total number of bypass links is close to the number of existing links. Additionally, theoretical analysis has been conducted only for uncorrelated networks (Park and Hahn 2016; Park et al. 2019). As mentioned above, degree correlation strongly affects network robustness. Therefore, this effect should be considered, as many real-world networks exhibit degree correlation.

The goal of this study was to reveal the relationship between the number of bypass links as a form of cost and the enhancement of network robustness. We introduce link-limited bypass rewiring, in which bypass links are connected stochastically. Our analytical and numerical results demonstrate that a network becomes more robust when additional bypass links are constructed in both uncorrelated and correlated scale-free networks. Furthermore, through numerical simulations using real-world network data, we determined that reconnecting nodes with higher degrees as bypass links makes networks more robust.

Node removals and robustness measures

As instances of random failures and targeted attacks, we consider node removals using probability. In node removal, a node with degree k is removed with a probability θ_k. When a network with degree distribution p_k is attacked via node removal with θ_k, the average removal probability θ is

$$\theta = \sum_{k=0}^{\infty} p_k \theta_k. \tag{1}$$

A random failure is one in which all nodes are removed with an equal probability ($\theta_k = \theta$), whereas a targeted attack removes nodes with higher degrees. In a targeted attack, the removal probability is

$$\theta_k = \begin{cases} 1 & (k > k') \\ N^*_{k'}/N_{k'} & (k = k') \\ 0 & (k < k'), \end{cases} \tag{2}$$

where k' is the maximum degree of the remaining nodes and $N^*_{k'}/N_{k'}$ is the fraction of the removed nodes whose degree was k' before the attack.

In this study, we consider the network robustness based on the size of the giant component S, which is the largest connected component of the network. The giant component is used as a robustness measure assuming that the network connectivity supports its functionality. In the analysis results, we used the percolation threshold θ_c, which is the fraction of removed nodes when the size of the giant component becomes zero ($S = 0$) in infinite networks in the percolation analysis (Cohen et al. 2000, 2001). The percolation threshold θ_c ranges from zero to one, where $\theta_c = 1$ indicates optimal robustness.

Because the percolation threshold θ_c cannot be accurately obtained through numerical simulations as a result of finite-sized effects, we used the robustness index R_{TA} (Schneider et al. 2011) in the numerical results. The robustness index against targeted attacks is defined as

$$R_{\mathrm{TA}} = \frac{1}{N} \sum_{q=1}^{N} \frac{S(q)}{N}, \tag{3}$$

where N is the number of nodes and $S(q)$ is the size of the giant component when q nodes are removed. The robustness index R_{TA} ranges from $1/N$ to 0.5. Both the percolation threshold θ_c and robustness index R_{TA} are calculated considering the size of the giant component relative to the fraction of removed nodes, and in many cases, these two indicators tend to be similar.

Concept of link-limited bypass rewiring

We propose link-limited bypass rewiring to alleviate the issues associated with node removals caused by random failures and targeted attacks. Figure 1 illustrates the concept of link-limited bypass rewiring. When a node is removed, its neighboring node is connected to another neighboring node. This new reconnected link is called a bypass link. When the degree of the removed node is odd, one neighboring node is not reconnected by a bypass link. In bypass rewiring (Park and Hahn 2016), all node pairs are connected by a new bypass link, whereas in link-limited bypass rewiring, each node pair is connected with a probability α_k, where k is the degree of the removed node. By making this process stochastic, the number of added bypass links can be controlled. For simplicity, we denote $\alpha_k = \alpha$ when α_k is a constant. For $\alpha = 0$, no rewiring is performed and for $\alpha = 1$, all node pairs are connected, which is equivalent to bypass rewiring.

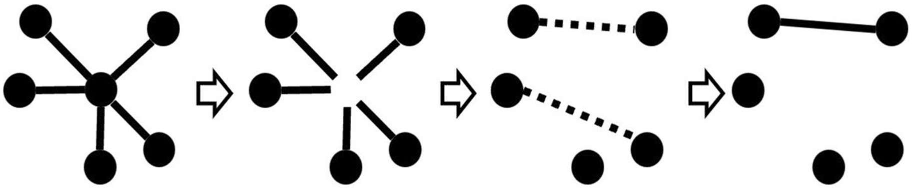

Fig. 1 Illustration of link-limited bypass rewiring with $\alpha = 0.5$. From the left in the figure, (1) a network before removal, (2) a node is removed, (3) node pairs are randomly selected, and (4) each link is connected with a probability $\alpha = 0.5$

There are various ways to select node pairs in link-limited bypass rewiring. We discuss random selection in the following section and compare various selection methods in the numerical simulation section.

Analytical results

In this section, we present a formalism for calculating the size of a giant component under link-limited random bypass rewiring. By using generating function methods, analytical solutions have been derived for random failures and targeted attacks (Cohen et al. 2000, 2001; Newman et al. 2001), and for random bypass rewiring (Park and Hahn 2016; Park et al. 2019). The analytical framework is a mean-field approximation method that can be applied to percolation processes on ensembles of locally tree-like networks with a given degree distribution. It cannot be applied to specific networks such as synthetic or real-world networks. Therefore, we focus on scale-free networks with a power-law degree distribution that are vulnerable to attacks and extend this framework to link-limited bypass rewiring.

Framework of bypass rewiring

Considering a random network with a degree distribution p_k subjected to node removals with a probability θ_k, the size of the giant component S is derived as follows (Cohen et al. 2000, 2001; Newman et al. 2001):

$$S = \sum_{k=0}^{\infty} p_k (1 - \theta_k)(1 - u^k), \tag{4}$$

where u is the average probability that a randomly selected node is not connected to the giant component According to previous studies (Cohen et al. 2000, 2001; Newman et al. 2001), we can calculate u as the minimum positive root of the self-consistent condition equation

$$u = \sum_{k=0}^{\infty} q_k (1 - \theta_{k+1}) u^k + \sum_{k=0}^{\infty} q_k \theta_{k+1}. \tag{5}$$

Here, q_k is the probability that a node following a randomly selected link has a degree $k + 1$.

$$q_k = \frac{(k+1)p_{k+1}}{\langle k \rangle} \tag{6}$$

Here, $\langle k \rangle$ is the average degree. By solving Eq. 5 numerically through fixed-point iteration, the size of the giant component S can be calculated from Eq. 4.

By extending the above formalism, the size of the giant component under random bypass rewiring has been derived (Park and Hahn 2016; Park et al. 2019). The basic concept of the associated formulation is illustrated in Fig. 2a. When the node following a randomly selected link is of degree $k = 2$ as q_1, it has only two patterns. The node is either not removed $(1-\theta_2)q_1$ or is removed and bypassed $\theta_2 q_1$. When the degree of a removed node is odd, one neighboring node remains unconnected to a bypass link. Therefore, the case in which a node cannot reach the connected component should be considered. When the node following a randomly selected link is of degree $k = 3$ as q_2, it has three patterns. The node is either not removed $(1-\theta_3)q_2$, removed and bypassed $2/3\theta_3 q_2$, or removed and not bypassed $1/3\theta_3 q_2$. Therefore, for random bypass rewiring, the condition equation is (Park and Hahn 2016)

$$\begin{aligned} u =& q_0(1-\theta_1) + q_0\theta_1 \\ &+ q_1(1-\theta_2)u + q_1\theta_2 u \\ &+ q_2(1-\theta_3)u^2 + \frac{2}{3}q_2\theta_3 u + \frac{1}{3}q_2\theta_3 + \cdots \end{aligned} \tag{7}$$

$$u = \sum_{k=0}^{\infty} q_k(1-\theta_{k+1})xu^k + u\sum_{k=0}^{\infty} q_k\theta_{k+1} + (1-u)\sum_{k=0}^{\infty}\frac{p_{2k+1}\theta_{2k+1}}{\langle k \rangle}. \tag{8}$$

By solving Eqs. 4 and 8, we can calculate the size of the giant component S for random bypass rewiring.

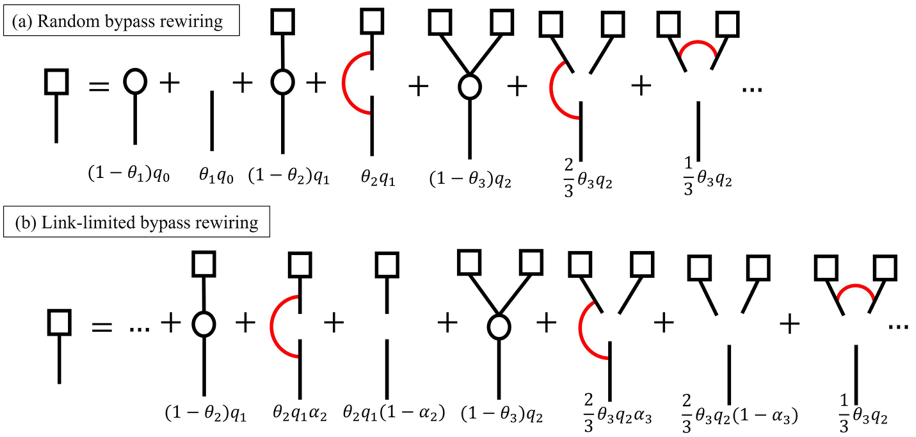

Fig. 2 Schematic representation of calculating the probability of reaching the connected component (square) for a node following a randomly selected link for **a** random bypass rewiring and **b** link-limited bypass rewiring. The circles represent nodes and red links are bypassed links. **a** Colored version of the diagram presented in Park and Hahn (2016)

Link-limited bypass rewiring for uncorrelated networks

Here, we derive the formalism of link-limited bypass rewiring in random networks with a degree distribution p_k. A schematic representation of link-limited bypass rewiring is presented in Fig. 2b. For link-limited bypass rewiring, each candidate link is connected with a probability α_k. When the node following a randomly selected link is of degree $k = 2$, it has three patterns. The node is either not removed $(1 - \theta_2)q_1$, removed and bypassed $\theta_2 q_1 \alpha_2$, or removed and not bypassed $\theta_2 q_1 (1 - \alpha_2)$. When the degree of the removed node is odd, the outcome is the same as that in random bypass rewiring. The condition equation for link-limited bypass rewiring is

$$\begin{aligned}u =& q_0(1-\theta_1) + q_0\theta_1 \\ &+ q_1(1-\theta_2)u + q_1\theta_2 u\alpha_2 + q_1\theta_2(1-\alpha_2) \\ &+ q_2(1-\theta_3)u^2 + \frac{2}{3}q_2\theta_3 u\alpha_3 + \frac{2}{3}q_2\theta_3(1-\alpha_3) + \frac{1}{3}q_2\theta_3 \\ &+ \cdots\end{aligned} \tag{9}$$

$$\begin{aligned}u =& \sum_{k=0}^{\infty} q_k(1-\theta_{k+1})xu^k + u\sum_{k=0}^{\infty} q_k\theta_{k+1}\alpha_{k+1} \\ &+ \sum_{k=0}^{\infty} q_k\theta_{k+1}(1-\alpha_{k+1}) + (1-u)\sum_{k=0}^{\infty}\frac{1}{\langle k\rangle}p_{2k+1}\theta_{2k+1}\alpha_{2k+1}.\end{aligned} \tag{10}$$

Therefore, the size of the giant component S under node removal with θ_k is calculated using Eqs. 4 and 10 for link-limited bypass rewiring.

The analytical solution for random bypass rewiring reveals that S with random bypass rewiring is greater than or equal to S without random bypass rewiring (Park and Hahn 2016). The same can be said for with link-limited bypass rewiring, allowing for further discussion. To calculate the condition equation, we can use fixed-point iteration. Let $f(u, \alpha_k)$ be the function on the right side of Eq. 10. Assuming that $\alpha_k = \alpha$ and $\beta_k = \beta$, an iteration is defined as

$$\begin{aligned}u_{i+1,\alpha} =& f(u_{i,\alpha}, \alpha) \\ u_{i+1,\beta} =& f(u_{i,\beta}, \beta),\end{aligned}$$

where i is the iteration step and $\alpha < \beta$. When the initial values are the same for $u_{0,\alpha} = u_{0,\beta} = 0$, $f(u_{i,\alpha}, \alpha) \leq f(u_{i,\beta}, \beta)$ for any i. Therefore, S with link-limited bypass rewiring increases as the probability α increases.

Figures 3 and 4 present the network fractions of the giant component under random failures and targeted attacks with link-limited bypass rewiring in a scale-free network. We present both the results of numerical simulations and the analytical results calculated using Eqs. 4 and 10. The scale-free network was generated using a configuration model with a degree distribution $p_k \propto k^{-3}$, $N = 20{,}000$ nodes, and average degree $\langle k\rangle \approx 3.5$.

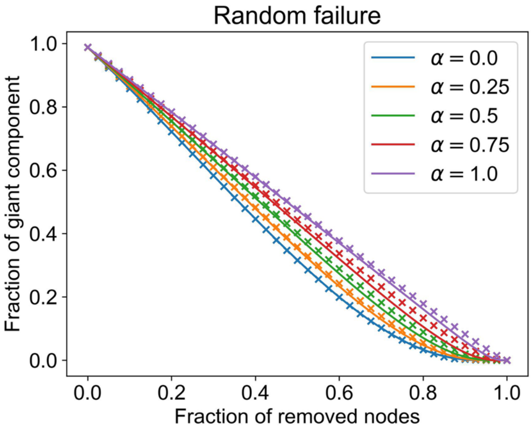

Fig. 3 Random failures with link-limited bypass rewiring in a scale-free network. Solid lines and crosses represent analytical and numerical results, respectively

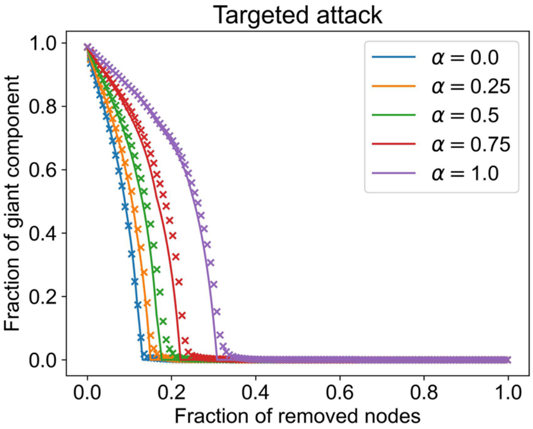

Fig. 4 Targeted attacks with link-limited bypass rewiring in a scale-free network. Solid lines and crosses represent analytical and numerical results, respectively

In Figs. 3 and 4, the size of the giant component increases as the probability α increases for both targeted attacks and random failures, which is consistent with the discussion above. For the random failures in Fig. 3, nearly optimal robustness with the percolation threshold $\theta_c = 0.99$ is obtained for $\alpha = 1$, whereas $\theta_c = 0.92$ for $\alpha = 0$. In other words, the scale-free network is sufficiently robust against random failures without bypass rewiring, but its robustness is nearly optimal when random bypass rewiring is applied. For the targeted attacks in Fig. 4, the percolation threshold $\theta_c = 0.31$ for $\alpha = 1$, whereas $\theta_c = 0.13$ for $\alpha = 0$. Compared to random failures, scale-free networks are more vulnerable to targeted attacks, even with random bypass rewiring. Therefore, in the following sections, we focus on targeted attacks.

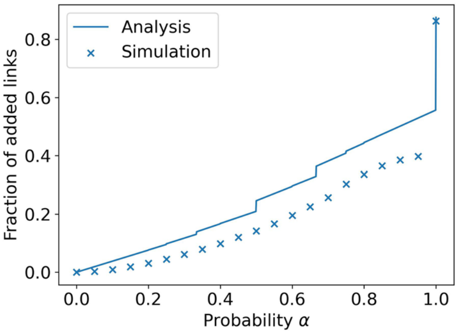

Fig. 5 Fraction of added bypass links relative to the numbers of original links in the scale-free network in the presence of targeted attacks with link-limited bypass rewiring. The analysis results were calculated using Eq. 11

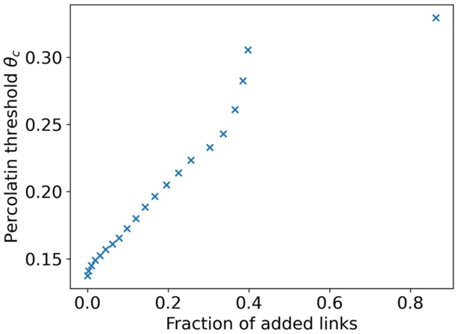

Fig. 6 Percolation threshold in the presence of targeted attacks versus the fraction of added bypass links in a scale-free network

Figure 5 presents the relationship between the probability α and percolation threshold θ_c in the presence of targeted attacks. When $\alpha < 1$, the number of added bypass links gradually increases as the probability α increases. At approximately $\alpha = 1$, the number of added bypass links increases steeply up to 80% of the existing links. For targeted attacks, the total number of added bypass links is approximately calculated as

$$n_{\text{total}} = \sum_{i=1}^{N} \left\lfloor \frac{\sum_{j \in \partial i} \alpha + (1-\alpha)\text{sign}(k_i - k_j)}{2} \right\rfloor, \tag{11}$$

where $j \in \partial i$ denotes the neighboring nodes of node i, $\lfloor x \rfloor$ is a floor function that returns the maximum integer less than or equal to x, and sign(x) returns $x = 1$ for $x > 0$ and $x = 0$ for $x \leq 0$. Inside the floor function is the expected degree of node i when removed by targeted attacks. The links connected to nodes with degrees $k_j \geq k_i$ are removed with a probability α. Note that the results are slightly overestimated because the case in which the added bypassed links are removed is not included.

Figure 6 reveals that as the number of bypassed links increases, the percolation threshold θ_c in the presence of targeted attacks increases. Therefore, when applying a framework of bypass rewiring to a real-world network, it is necessary to consider the balance between the cost of connecting bypass links and required network robustness.

Link-limited bypass rewiring for correlated networks

In this subsection, we describe link-limited bypass rewiring for degree-correlated networks. We begin with a correlated network with a joint degree-degree probability matrix $P(k, k')$, which contains the probabilities of randomly selecting links between nodes with degrees k and k'. The conditional probability $P(k|k') = P(k, k')/\sum_{k'} P(k, k')$ is the probability that a randomly selected link from a node with degree k' leads to a node with degree k. By using the conditional probability $P(k|k')$, we can calculate the size of the giant component with link-limited bypass rewiring in a correlated network.

Let x_k be the probability that a randomly selected link from a node with degree k is not connected to the giant component. The size of the giant component S with node removal θ_k and without bypass rewiring is calculated as Goltsev et al. (2008), Tanizawa et al. (2012)

$$S = \sum_{k=0}^{\infty} P(k)(1-\theta_k)(1-(x_k)^k), \tag{12}$$

$$x_k = \sum_{m=0}^{\infty} P(m|k)(1-\theta_m)x_m^{m-1} + \sum_{m=0}^{\infty} P(m|k)\theta_m. \tag{13}$$

When comparing Eqs. 5 and 13, one can see that q_k in Eq. 5 corresponds to $P(m|k)$ in Eq. 13. Similar to the above discussion, the condition equation for link-limited bypass rewiring in correlated networks can be derived as follows:

$$\begin{aligned} x_k = &\sum_{m=0}^{\infty} P(m|k)(1-\theta_{m+1})x_m^{m-1} \\ &+ \sum_{m=0}^{\infty} P(m|k)\theta_m \alpha_m x_m \\ &+ \sum_{m=0}^{\infty} P(m|k)\theta_m(1-\alpha_m) \\ &+ \sum_{m'=0}^{\infty} \frac{P(2m'+1|k)\theta_{2m'+1}(1-x_{2m'+1})}{2m'+1}\alpha_{2m'+1}. \end{aligned} \tag{14}$$

For correlated networks, we can calculate S using Eqs. 12 and 14.

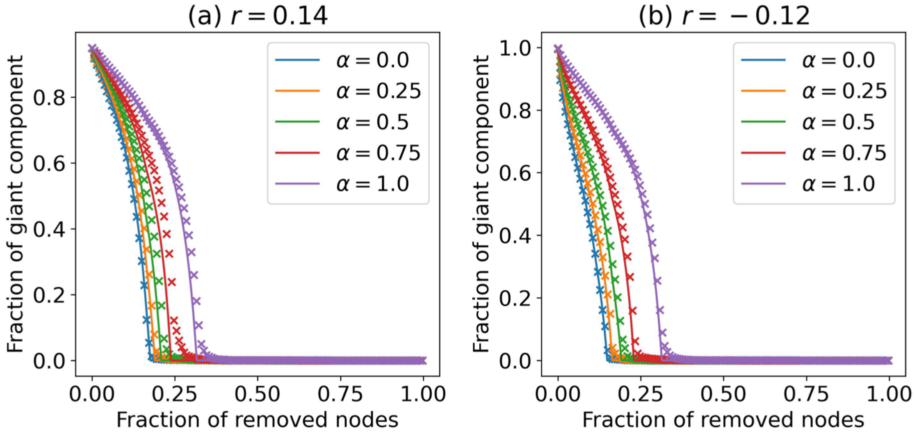

Fig. 7 Targeted attacks with link-limited bypass rewiring in a scale-free network with degree correlations **a** $r = 0.14$ and **b** $r = -0.12$. Solid lines and crosses represent analytical and numerical results, respectively

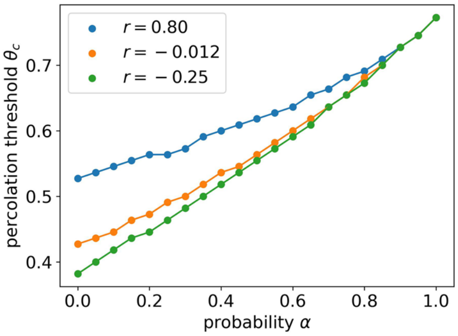

Fig. 8 Percolation threshold θ_c in the presence of targeted attacks for link-limited bypass rewiring with a probability α in bimodal networks. The degree correlations are $r = 0.8$, -0.012, and -0.25. As α increases, θ_c takes on a similar value, even for different degree correlations

Figure 7 presents the analytical and numerical results of link-limited bypass rewiring in a scale-free network with positive and negative degree correlations in the presence of targeted attacks. Networks with degree correlations were generated by performing random link swaps on random scale-free networks to increase (or reduce) degree correlation while maintaining the degree distribution. The original network had a degree correlation coefficient $r = -0.0094$ and the corresponding swapped network had a degree correlation coefficient $r = 0.14$ (or $r = -0.12$). Here, the degree correlation coefficient r is the correlation coefficient of the degree between linked nodes in the network (Newman 2002). For networks with degree correlations, the analytical and numerical simulation results exhibited similar values. Similar to the uncorrelated networks, the percolation threshold θ_c increased with α in the correlated networks.

We compared the percolation thresholds θ_c for different degree correlations. For $\alpha = 0$ without rewiring, the positive correlation was $\theta_c = 0.177$ and the negative correlation was $\theta_c = 0.150$. Similar to the results of previous studies (Schneider et al. 2011; Tanizawa et al. 2012), our findings indicate that networks with positive degree correlations are more robust against attacks. However, as α increased, the difference in θ_c decreased. In particular, for $\alpha = 1$, the positive correlation was $\theta_c = 0.320$ and

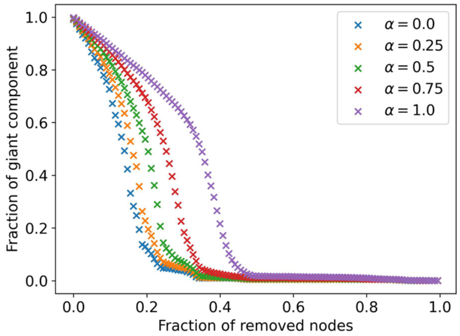

Fig. 9 Targeted attacks when using link-limited bypass rewiring with random selection in the Airtraffic network. Crosses represent numerical results

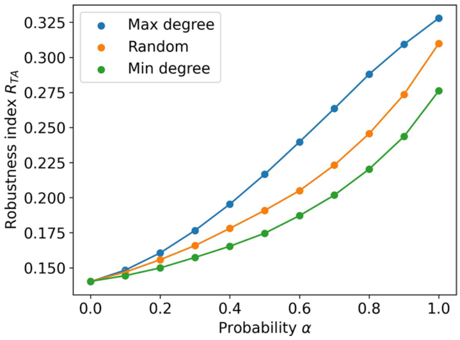

Fig. 10 Robustness index in the presence of targeted attacks when using link-limited bypass rewiring with different selection methods. Maximum-degree selection is the most effective approach in terms of improving robustness

the negative correlation was $\theta_c = 0.316$. Therefore, for a larger α, the influence of the degree correlation on the improvement in robustness decreases.

To highlight the effect of degree correlation more clearly, we also compared bimodal networks consisting of two degrees. Bimodal networks can alter their degree correlations (Mizutaka and Tanizawa 2016). We used bimodal networks consisting of 1000 nodes with degree three and 100 nodes with degree eight, and their degree correlations were $r = 0.80, -0.012$, and -0.25. Figure 8 presents the percolation thresholds θ_c of the analytical results. In Fig. 8, for $\alpha = 0$ without rewiring, θ_c has higher values for positive degree correlations r. However, as α increases, θ_c takes on a similar value and for $\alpha = 1$, θ_c has almost the same value. Similar to scale-free networks, the influence of the degree correlation in θ_c decreases for a larger α.

Numerical simulations using real-world networks

We investigated the applicability of link-limited bypass rewiring to real-world networks through numerical simulations. We used AirTraffic network data with $N = 1226$ nodes and 2408 links (Kunegis 2013). The nodes and links represent airports and preferred routes, respectively. The largest connected component was extracted from the original data and transformed into an undirected network without self-loop links.

Although we assumed that all candidate link pairs were selected randomly in Sect. 4, there could be better selection strategies in terms of improving robustness. Therefore, we identified an effective link selection method for link-limited bypass rewiring. We compared three selection methods: (1) minimum-degree selection, (2) maximum-degree selection, and (3) random selection. Minimum- (or maximum-) degree selection selects the pair of nodes with the minimum (or maximum) degrees among the neighbors of the removed node to define a candidate link.

Figure 9 presents the results of targeted attacks on the AirTraffic network when using link-limited bypass rewiring with random selection. Similar to the analytical results for the scale-free network, the AirTraffic network was more robust when the probability α was large. Figure 10 presents the robustness index R_{TA} against targeted attacks for the different selection methods. As shown in Fig. 10, the maximum-degree selection method improves robustness more than the other methods. In contrast, minimum-degree selection is less robust than random selection. Therefore, robustness can be further improved by constructing bypass links for nodes with higher degrees. Similar results are obtained for synthetic networks, the Barabási–Albert model (Barabási and Albert 1999), and the Watts–Strogatz model (Watts and Strogatz 1998) (see Appendix B).

Discussion and conclusion

In this paper, we proposed link-limited bypass rewiring to improve network robustness against random failures and targeted attacks. In link-limited bypass rewiring, the neighboring nodes of a removed node are reconnected stochastically using bypass links. We derived the size of the giant component under node removal with link-limited bypass rewiring in both uncorrelated and correlated networks. Our analysis and numerical results revealed that the networks became more robust with a higher probability of adding bypass links. Therefore, it can be concluded that adding additional bypass links makes a network more robust. In a previous study, every possible bypass link was added for bypass rewiring (Park and Hahn 2016). Although bypass rewiring significantly improves robustness, it requires a large number of bypass links (approximately equal to 80% of the original links). However, in real-world networks, adding new links can be costly. We presented results for the tradeoff between cost and robustness, highlighting a proportional relationship between the percolation threshold, which is a measure of robustness, and the number of bypass links.

Additionally, we investigated an effective node pair selection method for link-limited bypass rewiring. Through numerical simulations using AirTraffic network data, the addition of bypass links to nodes with higher degrees was found to be effective in terms of improving robustness. Interestingly, for many methods of improving robustness against attacks, focusing on high-degree nodes is less effective. For link addition prior to node removal, adding links to nodes with lower degrees is effective for improving robustness (Schneider et al. 2011; Chujyo and Hayashi 2022). This approach improves robustness by maintaining connectivity between low-degree nodes because high-degree nodes are initially removed by attacks. In contrast, link-limited bypass rewiring, in which bypass links are added after a node is removed, creates dense subgraphs by connecting high-degree nodes, which can be considered to improve robustness. These results indicate that strategies vary depending on the method used to improve robustness against node removal. In particular, a few studies have improved network robustness through recovery after targeted attacks (Sun and Zeng 2017; Afrin and Yodo 2019), and continued progress in this area is expected.

The advantages and disadvantages of our proposed link-limited bypass rewiring compared to those of other methods are now discussed. A major advantage of our method is that it is based on bypass rewiring, which optimally improves robustness (Park and Hahn 2016; Park et al. 2019), thereby achieving sufficient robustness while considering rewiring costs. However, a disadvantage of our method is that it does not revert to the original network structure. Conventional recovery methods restore the removed nodes or links (Quattrociocchi et al. 2014; Hu et al. 2016; Sun and Zeng 2017; Huang et al. 2018; Afrin and Yodo 2019), whereas our proposed method connects the remaining nodes after node removal and does not restore the original structure. When several nodes with higher degrees in the scale-free network are removed and our method is applied, the degree distribution changes to a power-law distribution with a cut-off, and the hub nodes are not restored. In addition, if the network has a community structure, the original community structure is not fully restored. In many cases, nodes belonging to close communities tend to be connected using our method because it rewires neighboring nodes from the removed node. Therefore, our method cannot restore the original system structure and functionality but is effective for repairs to maintain temporary robustness after attacks. Another disadvantage is that the proposed method assumes that as soon as one node is removed, its neighbor can be wired. However, this will likely be difficult to achieve in many real-world networks, and our method therefore has a disadvantage in terms of its implementation. In addition, our method cannot be used in situations in which several nodes stop functioning almost simultaneously, such as earthquakes or power grid overload events. In such cases, our method is not applicable, and restoration methods are required after a major disruption (Quattrociocchi et al. 2014; Hu et al. 2016; Huang et al. 2018).

Finally, we will discuss some limitations and future directions. Although we derived analytical solutions for both uncorrelated and correlated networks, real-world networks have complex structures such as community and cluster structures, and the application of link-limited bypass rewiring to networks with more complicated structures is a challenging problem. Furthermore, additional work is required to cover multilayer networks because multiple infrastructures are interdependent. Additionally, the function of a real-world network is not only connectivity but also the transportation of people and goods. However, this study only considered the robustness of connectivity. Therefore, it is necessary to investigate network robustness not only in terms of structure but also dynamics. Finally, this study compared selection methods based on degrees through numerical simulations. However, there may be more effective selection methods. Because node pair selection must be performed for each node removal, it is expected that strategies with high computational costs will be less likely to be applied.

Appendix A Link-limited bypass rewiring against random failures

The main text discusses the results of targeted attacks, but here, we present several results of random failures. We show the size of the giant component against random failures on correlated networks (Fig. 11) and AirTraffic network (Fig. 12). In addition, Fig. 13 shows the difference in the robustness index R_{rand} against random failures between selection methods for AirTraffic networks.

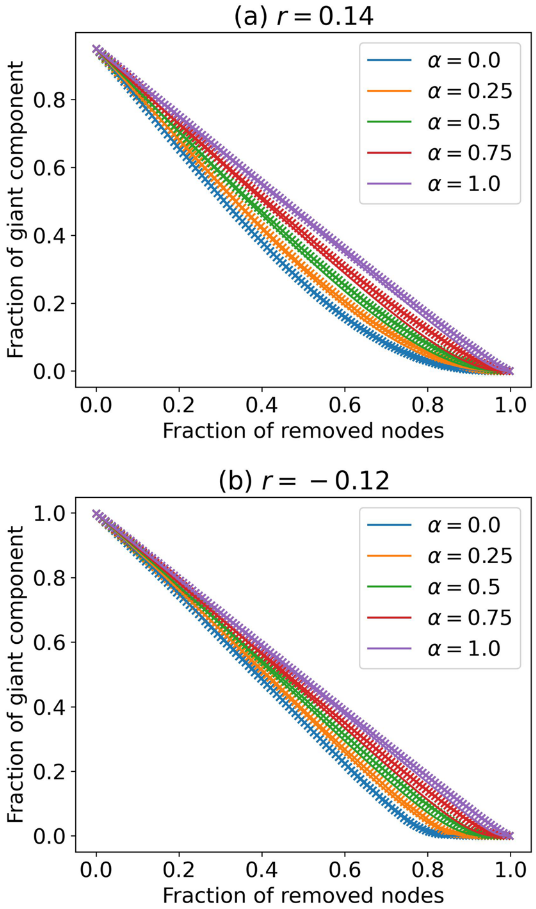

Fig. 11 Random failures with link-limited bypass rewiring in a scale-free network with degree correlations **a** $r = 0.14$ and **b** $r = -0.12$. Solid lines and crosses represent analytical and numerical results, respectively

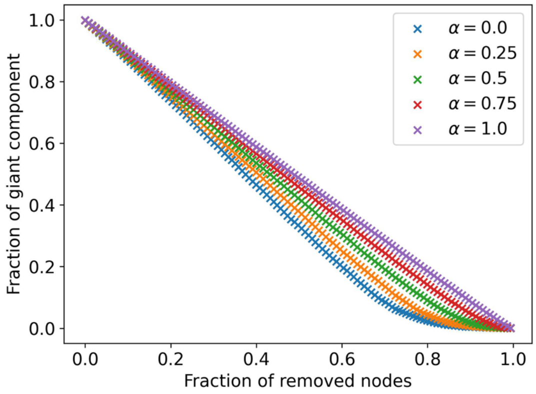

Fig. 12 Random failures when using link-limited bypass rewiring with random selection in Airtraffic network. Crosses represent numerical results

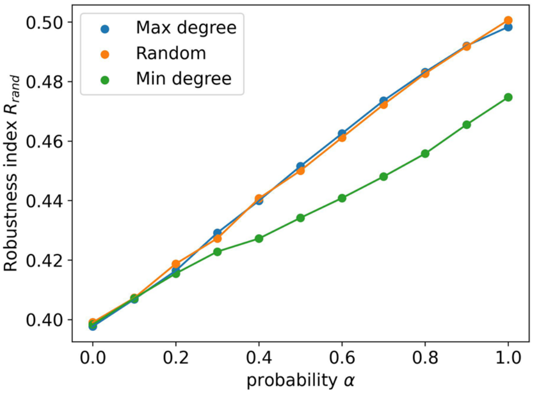

Fig. 13 Robustness index in the presence of random failures when using link-limited bypass rewiring with different selection methods

Appendix B Numerical results of network models

While the main text discusses the numerical results of air traffic data, this Appendix presents the numerical results of synthetic network models with similar trends. We used scale-free networks with 1000 nodes and 1996 links generated by the Barabási–Albert

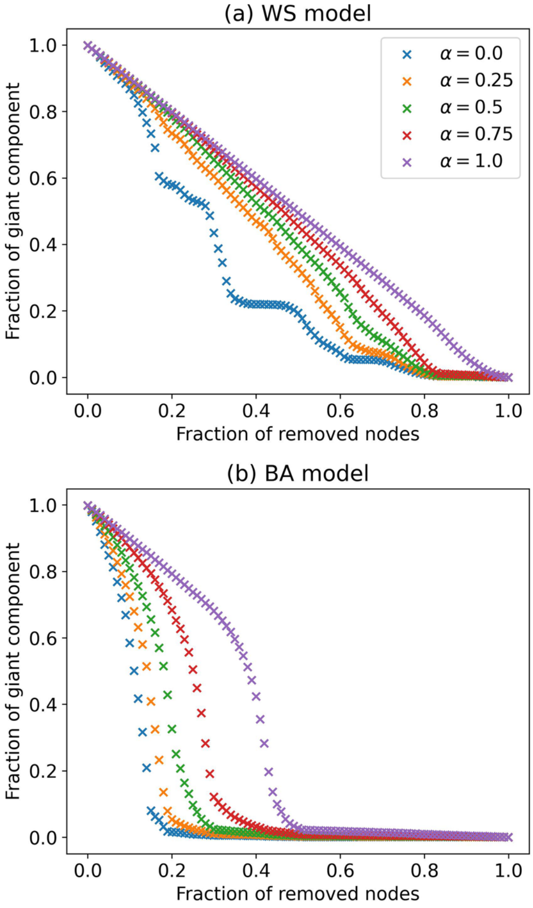

Fig. 14 Targeted attacks when using link-limited bypass rewiring with random selection in the **a** Watts–Strogatz model and **b** Barabási–Albert model. Crosses represent numerical results

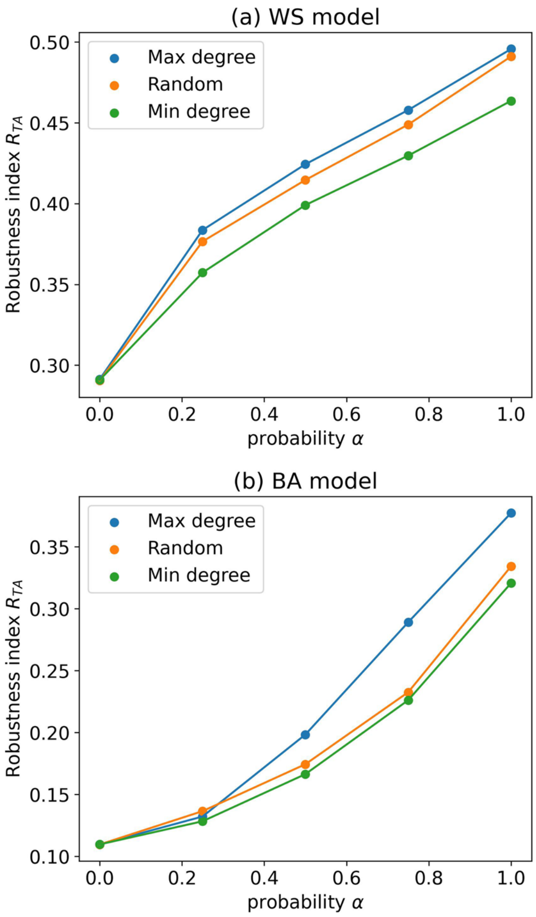

Fig. 15 Robustness index in the presence of targeted attacks when using link-limited bypass rewiring with different selection methods in the **a** Watts–Strogatz model and **b** Barabási–Albert model. Maximum-degree selection is the most effective approach in terms of improving robustness

model (Barabási and Albert 1999) and small-world networks with 1000 nodes, 2000 links, and rewiring probability $p = 0.1$ generated by the Watts–Strogatz model (Watts and Strogatz 1998). Figure 14 presents the results of targeted attacks on the synthetic networks when using link-limited bypass rewiring with random selection. Figure 15 presents the robustness index R_{TA} against targeted attacks for the different selection methods.

Acknowledgements
We would like to thank Editage (www.editage.jp) for English language editing.

Author contributions
MC derived equations and performed numerical simulations. MC and FT discussed the results and wrote the manuscript. All authors read and approved the final manuscript.

Funding
Partial financial support was received from TechnoPro Holdings, Inc. and Next Generation Artificial Intelligence Research Center, the University of Tokyo.

Data availability
The datasets analysed during the current study are available in the KONECT repository, http://konect.cc/networks/maayan-faa/.

Declarations

Conflict of interest

The authors declare that they have no Conflict of interest.

Received: 4 March 2024 Accepted: 13 May 2024
Published online: 23 May 2024

References

Afrin T, Yodo N (2019) A concise survey of advancements in recovery strategies for resilient complex networks. J Complex Netw 7(3):393–420
Albert R, Barabási A-L (2002) Statistical mechanics of complex networks. Rev Mod Phys 74(1):47
Albert R, Jeong H, Barabási A-L (2000) Error and attack tolerance of complex networks. Nature 406(6794):378–382
Barabási A-L, Albert R (1999) Emergence of scaling in random networks. Science 286(5439):509–512
Beygelzimer A, Grinstein G, Linsker R, Rish I (2005) Improving network robustness by edge modification. Physica A 357(3–4):593–612
Chan H, Akoglu L (2016) Optimizing network robustness by edge rewiring: a general framework. Data Min Knowl Discov 30:1395–1425
Chujyo M, Hayashi Y (2021) A loop enhancement strategy for network robustness. Appl Netw Sci 6(1):1–13
Chujyo M, Hayashi Y (2022) Adding links on minimum degree and longest distance strategies for improving network robustness and efficiency. PLoS ONE 17(10):0276733
Cohen R, Erez K, Ben-Avraham D, Havlin S (2000) Resilience of the internet to random breakdowns. Phys Rev Lett 85(21):4626
Cohen R, Erez K, Ben-Avraham D, Havlin S (2001) Breakdown of the internet under intentional attack. Phys Rev Lett 86(16):3682
Dorogovtsev SN, Goltsev AV, Mendes JF (2008) Critical phenomena in complex networks. Rev Mod Phys 80(4):1275
Goltsev AV, Dorogovtsev SN, Mendes JF (2008) Percolation on correlated networks. Phys Rev E 78(5):051105
Hayashi Y (2018) A new design principle of robust onion-like networks self-organized in growth. Netw Sci 6(1):54–70
Hu F, Yeung CH, Yang S, Wang W, Zeng A (2016) Recovery of infrastructure networks after localised attacks. Sci Rep 6(1):24522
Huang Y, Wu J, Ren W, Chi KT, Zheng Z (2018) Sequential restorations of complex networks after cascading failures. IEEE Trans Syst Man Cybern Syst 51(1):400–411
Kunegis J (2013) Konect: the Koblenz network collection. In: Proceedings of the 22nd international conference on world wide web, pp 1343–1350
Louzada VH, Daolio F, Herrmann HJ, Tomassini M (2013) Smart rewiring for network robustness. J Complex Netw 1(2):150–159
Mizutaka S, Tanizawa T (2016) Robustness analysis of bimodal networks in the whole range of degree correlation. Phys Rev E 94(2):022308
Newman ME (2002) Assortative mixing in networks. Phys Rev Lett 89(20):208701
Newman M (2018) Networks. Oxford University Press, Oxford
Newman ME, Strogatz SH, Watts DJ (2001) Random graphs with arbitrary degree distributions and their applications. Phys Rev E 64(2):026118
Park J, Hahn SG (2016) Bypass rewiring and robustness of complex networks. Phys Rev E 94(2):022310
Park J, Shin S, Hahn SG (2019) Bypass rewiring and extreme robustness of Eulerian networks. Physica A 515:324–331
Quattrociocchi W, Caldarelli G, Scala A (2014) Self-healing networks: redundancy and structure. PLoS ONE 9(2):87986
Schneider CM, Moreira AA, Andrade JS Jr, Havlin S, Herrmann HJ (2011) Mitigation of malicious attacks on networks. Proc Natl Acad Sci 108(10):3838–3841
Sun W, Zeng A (2017) Target recovery in complex networks. Eur Phys J B 90:1–6
Tanizawa T, Havlin S, Stanley HE (2012) Robustness of onion like correlated networks against targeted attacks. Phys Rev E 85(4):046109
Watts DJ, Strogatz SH (1998) Collective dynamics of 'small-world '. Nature 393(6684):440–442
Wu Z-X, Holme P (2011) Onion structure and network robustness. Phys Rev E 84(2):026106

Publisher's Note