

Title	A loop enhancement strategy for network robustness
Author(s)	Chujyo, Masaki; Hayashi, Yukio
Citation	Applied Network Science, 6: 3
Issue Date	2021-01-09
Type	Journal Article
Text version	publisher
URL	http://hdl.handle.net/10119/20001
Rights	Copyright (c) 2021 Author(s). Masaki Chujyo, Yukio Hayashi. This is an Open Access article distributed under the terms of Creative Commons Licence CC-BY [https://creativecommons.org/licenses/by/4.0/]. Original publication is available on Springer Nature via https://doi.org/10.1007/s41109-020-00343-6 .
Description	

RESEARCH

Open Access



A loop enhancement strategy for network robustness

Masaki Chujiyo^{*†} and Yukio Hayashi[†]

*Correspondence:

mchujiyo@jaist.ac.jp

[†]Masaki Chujiyo and Yukio Hayashi have contributed equally to this work
Japan Advanced Institute of Science and Technology,
1-1 Asahidai, Nomi, Ishikawa
932-1292, Japan

Abstract

Many real systems are extremely vulnerable against attacks, since they are scale-free networks as commonly existing topological structure in them. Thus, in order to improve the robustness of connectivity, several edge rewiring methods have been so far proposed by enhancing degree–degree correlations. In fact, onion-like structures with positive degree–degree correlations are optimally robust against attacks. On the other hand, recent studies suggest that the robustness and loops are strongly related to each other. Therefore, we focus on enhancing loops as a new approach for improving the robustness. In this work, we propose edge rewiring methods and evaluate the effect on the robustness by applying to real networks. Our proposed methods are two types of rewirings in preserving degrees or not for investigating the effect of the degree modification on the robustness. Numerical results show that our proposed methods improve the robustness to the level as same or more than the state-of-the-art methods. Furthermore, our work shows that the following two points are more important for further improving the robustness. First, the robustness is strongly related to loops more than degree–degree correlations. Second, it significantly improves the robustness by reducing the gap between the maximum and minimum degrees.

Keywords: Edge-rewiring, Robustness against attacks, Enhancing loops

Introduction

Improving robustness against malicious attacks has been one of the important issues in network science. Because many real networks are scale-free whose degree distributions follow power-law, and their connectivity is extremely vulnerable against removal of targeted nodes (Barabási and Albert 1999; Albert et al. 2000; Cohen et al. 2001). This vulnerability causes the loss of essential functions as networks in many real systems, which operate on the assumption that all nodes are connected.

For example, the following infrastructures were damaged by disasters, and caused significant impacts on our society. A massive ice storm in Eastern Canada caused a long-term blackout in 1998 (Chang et al. 2007). It reveals the strong dependence on electric power. Also, a power outage in the USA and Canada continued for two days in 2003, and caused transportation and economic disruptions (Minkel 2008). In 2008, a power grid network in China broken down due to heavy snowfall (Zhou and Liu 2016). On the other type of disasters, the eruption of Icelandic volcano Eyjafjallajökull in 2010 affected

European air traffic and stranded thousands of passengers (Brooker 2010). The earthquakes and tsunamis that struck Japan in 2011 caused a terrible loss of life and property further disrupting the global supply chain network (MacKenzie et al. 2012). In 2012, Hurricane Sandy destroyed the large areas in New York and New Jersey (Manuel 2013). After that, the blackout in several months affected the transportation network, and caused multiple damages (Lipton 2013). Thus, these infrastructures directly connected to our life have potential risks, and it is necessary to design a new structure to mitigate the outage.

They are also seriously damaged by attacks with targeting a specific part. For example, the North American power network is robust against failures, but its function is greatly reduced for targeted attacks (Albert et al. 2004). Moreover, an assessment of the urban rail transport network indicates that the Shanghai Metro is vulnerable to degree-based attacks (Sun et al. 2015). In investigating the robustness of the global air transport network against intentional attacks, the weak points are discussed in a viewpoint from each airport's centrality (Lordan et al. 2014). Furthermore, the robustness is analyzed against both failures and attacks of airline network routes in combining Low Cost Carriers (LCCs) and Full Service Carriers (FSCs) (Lordan et al. 2016). It is concluded that route networks of LCC are more robust than ones of FSC.

Since many of the above infrastructures in daily life have vulnerability against attacks, several methods should be developed for improving the robustness of connectivity in network systems. We remark that such systems can be more robust by partial edge rewiring without adding new resources of edges (Schneider et al. 2011). Thus, we aim to improve the robustness without adding any resources in assuming that the number of both nodes and edges is constant. Particularly, the edges in the airline network or the wireless communication network can be easily changed as rewiring. The rewiring with preserving degrees in the airport network or wireless communication is possible by changing the destination of the airport or the direction of the wireless beam. In contrast, it may be difficult to change the network structure when edges are spatially embedded, such as road networks, water supply networks, and power grid networks. However, even on such systems, it will be useful for maintaining network functions to make the robust structure by adding new resources or renovating and rebuilding.

Although we discuss the robustness of connectivity by attacks, we may consider other attacks. Some edge rewiring algorithms have also been proposed as adversarial attacks against link prediction (Yu et al. 2019) and community detection (Chen et al. 2019). While they aim to rewire the connections for privacy protections, we aim to enhance the tolerance of connectivity against node removals.

On the other hand, an onion-like structure with positive degree–degree correlations (Newman 2002) is optimally robust against targeted attacks under a given degree distribution (Schneider et al. 2011; Tanizawa et al. 2012). The degree–degree correlations r is defined as the Pearson correlation coefficient for degrees at both ends of an edge (Newman 2002). The onion-like structure is visualized by arranging similar degree nodes on a concentric circle in decreasing order of degrees from the core to the peripheral. Since similar degree nodes tend to be connected by the positive degree–degree correlations, they draw a circle. It can be generated by greedy rewiring to maximize a robustness index R_{hub} , which accumulates the size of the largest connected component after attacks

(Schneider et al. 2011). The robustness index R_{hub} is defined as $R_{\text{hub}} = \frac{1}{N} \sum_{q=1/N}^1 S(q)$, where $S(q)$ denotes the number of nodes included in the largest connected component after removing qN nodes, and q is the fraction of removal nodes by high degree adaptive attacks. However, there is no strict definition of an onion-like structure for the thresholds of R_{hub} or r , since too high degree–degree correlations rather decrease the robustness (Schneider et al. 2011; Tanizawa et al. 2012; Murakami et al. 2017). Thus, through numerical simulations, it is considered that the onion-like networks have $R_{\text{hub}} > 0.3$ and $r > 0.2$ because not onion-like scale-free networks by Barabási-Albert model (Barabási and Albert 1999) have $R_{\text{hub}} < 0.23$ and $r \approx 0$ at the same size (Hayashi and Uchiyama 2018). The values of R_{hub} and r for onion-like networks are also obtained by rewiring for enhancing degree–degree correlations (Wu and Holme 2011). Note that the R_{hub} represents the area under the curve $S(q)/N$ versus $q = \frac{1}{N}, \frac{2}{N}, \dots, \frac{N-1}{N}, 1$, and can take different values for networks with the same critical point q_c for whole fragmentation. In other words, the R_{hub} takes a large value when $S(q)$ decreases steeply at q_c , whereas it takes a small value when $S(q)$ decreases gently even at the same q_c .

Based on enhancing the degree–degree correlations, several rewiring methods have been proposed for improving the robustness (Xulvi-Brunet and Sokolov 2002; Wu and Holme 2011). However, in recent years, an incrementally growing method is also proposed for constructing an onion-like network by enhancing loops (or cycles in graph theory) instead of the degree–degree correlations (Hayashi 2018; Hayashi and Uchiyama 2018). It has been suggested that there is a strong relation between robustness and loop structure.

In this work, we propose new rewiring methods to enhance loops, and discuss the topological structures in improving the robustness for real data of the infrastructure networks. We emphasize the relation between robustness and loop rather than the conventional degree–degree correlations.

Methods

We explain our motivations for the rewiring strategy in enhancing loops. Several methods have been so far proposed for improving the robustness to be an onion-like structure by increasing the degree–degree correlations (Xulvi-Brunet and Sokolov 2002; Wu and Holme 2011). However, a network with the extremely high degree–degree correlations is not the best (Schneider et al. 2011; Tanizawa et al. 2012; Murakami et al. 2017). Therefore, for the improvement of robustness, there may exist other approaches instead of the degree–degree correlations.

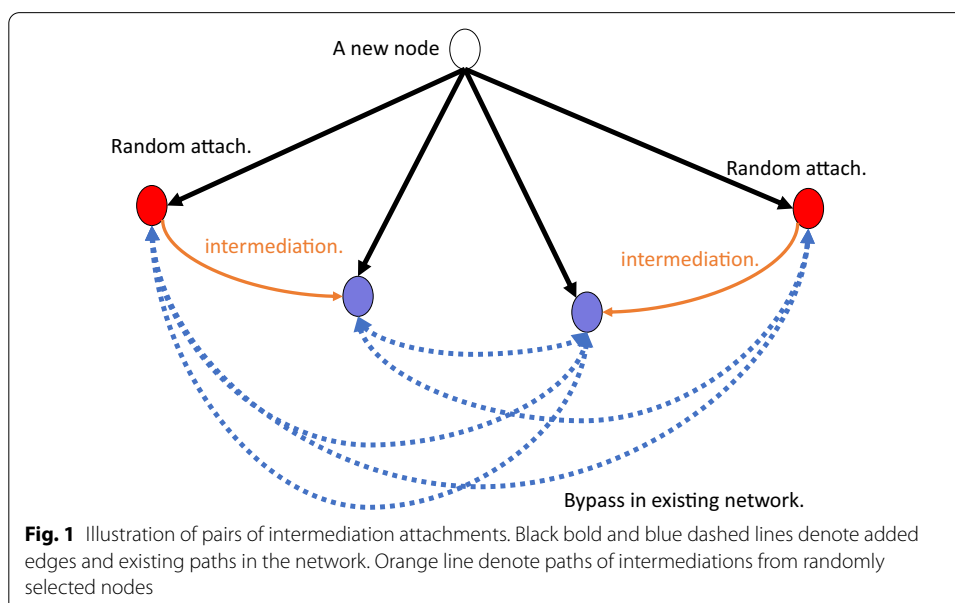
We remark a strong relation of robustness and loops from some suggesting works (Braunstein et al. 2016; Hayashi and Uchiyama 2018). One of them is the equivalence of network dismantling and decycling problems (Braunstein et al. 2016). Here, network dismantling problem is finding a minimum set of nodes that removal makes the network broken into connected components at most a given size. Network decycling problem is finding a minimum set of nodes that removal makes the network without loops. The decycling set is named as Feedback Vertex Set (FVS) in computer science. The equivalence means that networks become a tree structure at the critical point before the whole fragmentation. Therefore, in order to avoid fragmentation, it is necessary not to be a tree as long as possible against node removals. On the other hand, the relation of the

robustness and loops is also discussed in generating the onion-like structure with the optimal tolerance of connectivity against attacks. In the generation based on a pair of random and intermediation attachments, a new node links to a randomly selected node and the minimum degree node in distant neighbors through a few hops of intermediation from the randomly selected pair node (Hayashi and Uchiyama 2018). We intuitively understand that many loops with bypasses are formed by pairs of attachments as shown in Fig. 1. In fact, it is found that the robustness index R_{hub} and the size of FVS have strong correlations in the networks.

Focusing the above correlations, we propose a new edge rewiring strategy for enhancing loops in two types: Preserving and Non-preserving with modification of the degree distribution. As similar to the conventional methods, in Preserving, the rewiring does not change each node's degree under the original degree distribution. However, in Non-preserving, the rewiring changes degrees and the degree distribution in order to investigate the effect of changes in the degree distribution on robustness.

Spanning trees and the fundamental cycles

The fundamental system of cycles (loops) in a spanning tree is known in graph theory. A spanning tree is a subgraph that all nodes of the network are connected without loops. The chords are edges not belonging in the spanning tree. Each chord and a loop called a fundamental cycle are one-to-one correspondings (Bollobás 2013). In other words, a spanning tree has $M - N + 1$ fundamental cycles as a linearly independent basis, where M and N denote the numbers of edges and nodes. Therefore, any loop is represented as a combination of the basis. It is expected that there are many loops independently on networks with a large number of spanning trees. Independently from the above our explanation, a rewiring method for increasing the number of spanning trees has been proposed by applying the perturbation theory of the Laplacian matrix (Chan and Akgolu 2016). The authors consider a rewiring in Preserving by the addition and removal of



edges based on the Kirchhoff's matrix-tree theorem (Buekenhout and Parker 1998). In contrast, we consider the edge rewiring strategy to enhance loops by increasing the size of Feedback Vertex Set instead of the number of spanning trees.

Feedback vertex set

Since the Feedback Vertex Set (FVS) is the minimum set of nodes whose removal makes the network acyclic, the remaining trees after removing the FVS are easily fragmented by further removal. The attack method to a node estimated in the FVS by Belief Propagation is proposed (Mugisha and Zhou 2016). Inversely, it is expected that increasing the size of FVS leads to improve the robustness of connectivity against node removal.

For increasing the size of FVS, we propose a new rewiring strategy by enhancing loops to improve the robustness. Since to find the FVS belongs to a class of NP-hard combinatorial optimization problems, the exact solution is intractable for a large network. Therefore, we apply an approximation algorithm of Belief Propagation (BP) in statistical physics (Zhou 2013). The algorithm estimates the probability q_i^0 belonging to FVS for node i . Here, $q_i^{A_i}$ denotes the marginal probability for node i 's root: $A_i = 0$ (empty) or $A_i = i$ (the root is itself). When the node is empty, it is unnecessary as a root so that it is estimated as belonging to the FVS. Based on a cavity method (Zhou 2013; Mugisha and Zhou 2016), the explicit formulas are

$$q_i^0 = \frac{1}{z_i}, \quad (1)$$

$$z_i = 1 + e^x \left[1 + \sum_{k \in \partial i} \frac{1 - q_k^0}{q_{k \rightarrow i}^0 + q_{k \rightarrow i}^k} \right] \prod_{j \in \partial i} [q_{j \rightarrow i}^0 + q_{j \rightarrow i}^j], \quad (2)$$

where ∂i denotes node i 's set of neighbor nodes, $x > 0$ is a parameter of inverse temperature, and z_i is normalization constant. The $q_{i \rightarrow j}^0$ and $q_{i \rightarrow j}^i$ are calculated from the following self-consistent BP equations,

$$q_{i \rightarrow j}^0 = \frac{1}{z_{i \rightarrow j}}, \quad (3)$$

$$q_{i \rightarrow j}^i = \frac{e^x \prod_{k \in \partial i \setminus j} [q_{k \rightarrow i}^0 + q_{k \rightarrow i}^k]}{z_{i \rightarrow j}}, \quad (4)$$

$$z_{i \rightarrow j} = 1 + e^x \prod_{k \in \partial i \setminus j} [q_{k \rightarrow i}^0 + q_{k \rightarrow i}^k] \times \left[1 + \sum_{l \in \partial i \setminus j} \frac{1 - q_{l \rightarrow i}^0}{q_{l \rightarrow i}^0 + q_{l \rightarrow i}^l} \right], \quad (5)$$

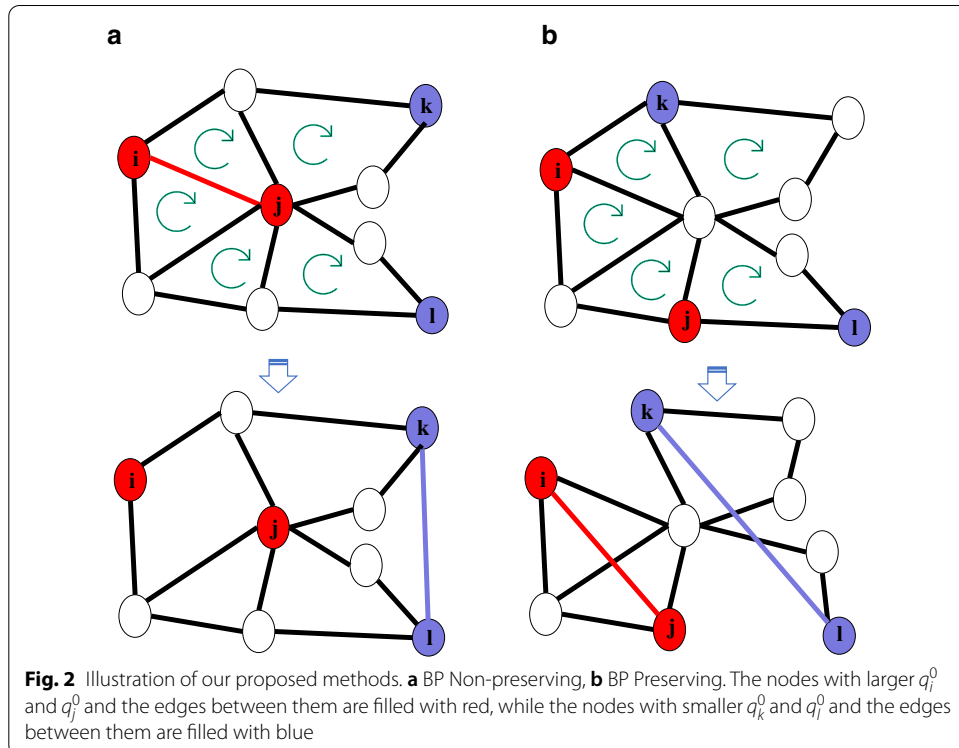
where $\partial i \setminus j$ denotes node i 's set of neighbor nodes except node j , and $z_{i \rightarrow j}$ is normalization constant. Equations (1)–(5) are iterated from an initial set of random values in $(0, 1)$ until given rounds in practically. In each round, a set $\{q_i^0 | i = 1, \dots, N\}$ are updated in order of random permutation of the all N nodes. To obtain the FVS, we remove a node i with a higher q_i^0 and recalculate a set $\{q_i^0\}$ for all existing nodes until given rounds. The removed nodes are estimated as the FVS. We repeat them until the network without

loops. A node i with a smaller q_i^0 is less related to loops. In other words, a node i with a smaller q_i^0 tends not to belong to FVS. Using this $\{q_i^0\}$, we consider the edge addition and deletion for increasing the size of FVS as follows.

BP Non-preserving

The following rewiring without preserving degrees is called BP Non-preserving. Here this rewiring modifies degrees under a constant number of nodes and edges. In BP Non-preserving, to increase the size of FVS, we add an edge (k, l) between nodes with smaller q_k^0 and q_l^0 in the all unconnected nodes pairs. It is expected to increase the size of FVS by adding the edge, since these nodes tend not to belong to any loops, and their connection makes a new loop. To keep the number of edges, we remove an edge (i, j) between nodes with larger q_i^0 and q_j^0 in the all connected nodes pairs. Removing the edge (i, j) has little impact on the size of FVS, since the nodes i and j are on many loops because of large q_i^0 and q_j^0 as candidates of FVS. As shown in Fig. 2a, the following steps are repeated in BP Non-preserving. Note that we may exchange steps 1 and 2 because they are independent processes.

- Step 1* Add a non-existing edge (k, l) with the minimum q_k^0 and q_l^0 .
- Step 2* Remove an edge (i, j) with the maximum q_i^0 and q_j^0 .
- Step 3* Recalculate $\{q_i^0 | i = 1, \dots, N\}$.



BP Preserving

The following rewiring with preserving degrees is called BP Preserving. As similar to Chan and Akoglu (2016), we apply the three steps: (1) add a non-existing edge (i, j) , (2) remove edges (i, k) and (j, l) , and (2) add a non-existing edge (k, l) . We illustrate the steps before and after rewiring at the top and bottom in Fig. 2b, respectively. It consists of the additions of two edges (i, j) and (k, l) , and the removal of two edges (i, k) and (j, l) in order to preserve degrees.

For increasing the size of FVS, it is effective to add two edges between nodes with smaller q_i^0 . However, it can not apply to BP Preserving, since the removal for preserving degrees in the above step (2) makes fragmentation. Nodes with smaller q_i^0 tend to have smaller degrees and belong to a tree. In the worst-case, when we select nodes i and j with degree one or on a dangling tree, they are isolated by the removal. To avoid it, we select two unconnected nodes i and j with larger q_i^0 and q_j^0 in all nodes at first, since they tend to have large degrees and removing edges emanated from them is not likely to decrease the connectivity. Then, we select unconnected nodes k and l with smaller q_k^0 and q_l^0 in the neighbors of nodes i and j , respectively, in order to enhance loops by connecting them in the above step (3). Since the nodes k and l are selected in the neighbors of nodes i or j , not in all nodes, they may be a little contained in loops, which is not the worst-case and prevents isolation. In this way, we first add an edge (i, j) between nodes i and j with larger q_i^0 and q_j^0 in avoiding fragmentation by rewiring as much as possible. These selections possibly increase the size of FVS, since the nodes k and l with smaller q_k^0 and q_l^0 are expected to be included in new loops. For the removal, we select edges (i, k) between nodes with larger q_i^0 and smaller q_k^0 , and (j, l) between nodes with larger q_j^0 and smaller q_l^0 . The removals have little impact on the size of FVS, since the edges linked to nodes with smaller q_k^0 or q_l^0 tend to belong to fewer loops. As shown in Fig. 2b, the following steps are repeated in BP Preserving.

- Step 1* Let (i, j) be a non-existing edge with the maximum q_i^0 and q_j^0 in a network.
- Step 2* Let k be a node with the minimum q_k^0 in the neighbor of either node i . Let l be a node with the minimum q_l^0 in the neighbor of node j but not the neighbor of node k .
- Step 3* Add non-existing edges (i, j) and (k, l) and remove edges (i, k) and (j, l) .
- Step 4* Recalculate $\{q_i^0 | i = 1, \dots, N\}$.

Results

In this section, we evaluate the effects of enhancing loops on the improvement of robustness in our proposed methods. Also, we discuss a relation between the robustness and the size of FVS. For comparison, Degree, WuHolme (Wu and Holme 2011), and SP (Chan and Akoglu 2016) are investigated. Degree is a modification of our rewiring strategy between nodes with smaller degrees instead of smaller q_i^0 of BP. It has two types: Degree Preserving and Degree Non-preserving, corresponding to BP Preserving and BP Non-preserving. We consider WuHolme as a baseline in Preserving, because it is the best conventional method for improving the robustness by

increasing the degree–degree correlations. SP is the previously mentioned method for increasing the number of spanning trees, and it also has two types: SP Preserving and SP Non-preserving. We compare it as a different approach in order to enhance loops.

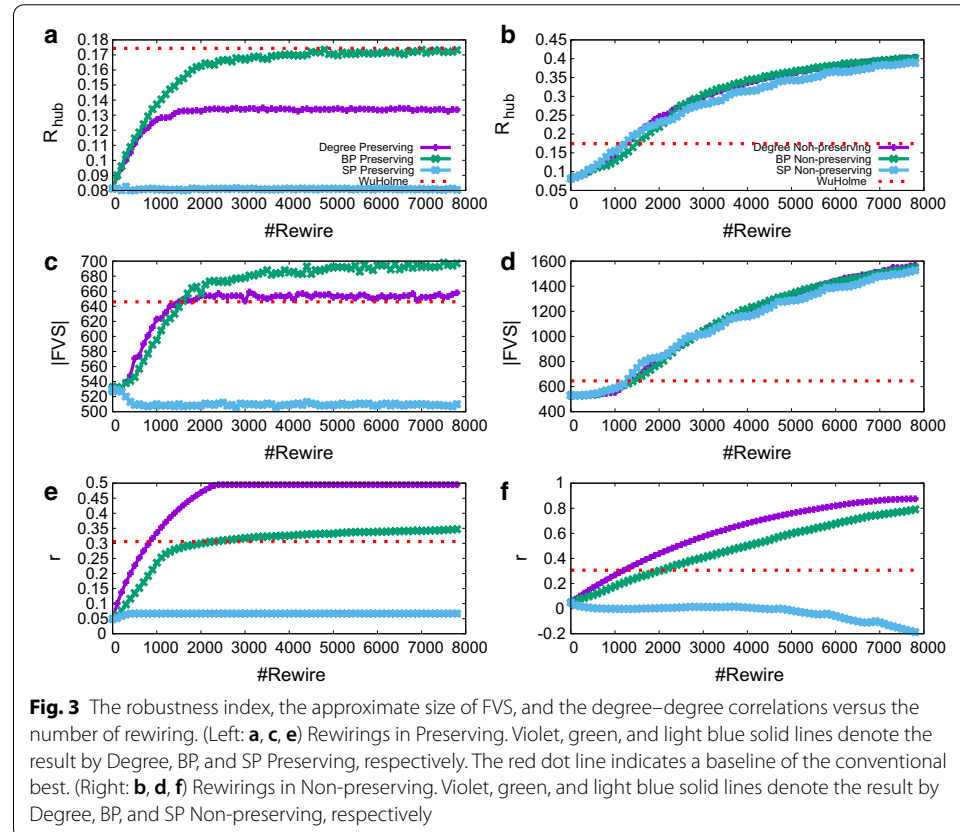
We apply our proposed and conventional methods for several real networks including social, biological, and technological networks, for which similar results are obtained (See Additional file 1). As a typical result, Fig. 3 shows the robustness index R_{hub} , the approximate size of FVS, and the degree–degree correlations r versus the number of rewirings for a real network: an airline network named OpenFlights with $N = 2905$ nodes and $M = 15,645$ edges (Kunegis 2013). The robustness index R_{hub} is the sum of the fraction of nodes in the largest connected component against high degree adaptive attacks with recalculation of degrees (Schneider et al. 2011). The degree–degree correlations r is the Pearson correlation coefficient for degrees (Newman 2002). In the following, $|FVS|$ denotes the size of FVS by Belief Propagation (Zhou 2013), and $\#Rewire$ is the number of rewirings. Note that almost all edges are rewired at $\#Rewire = 7800$, which is nearly half of M .

First, we show the results for our proposed BP Preserving. At the left in Fig. 3c, BP Preserving (denoted by the green line) increases up to $|FVS| = 698$ from the original $|FVS| = 528$ before rewiring at $\#Rewire = 0$. The rate of FVS rises from 18% to 24%. Since the baseline (denoted by the red dot line) is $|FVS| = 646$, BP Preserving increases $|FVS|$ over the baseline. Furthermore, at the left in Fig. 3a, BP Preserving (denoted by the green line) improves R_{hub} to almost the same as the baseline (denoted by the red dot line). The maximum R_{hub} is 0.175 in BP Preserving (denoted by the green line) and 0.174 in the baseline (denoted by the red dot line) at the left in Fig. 3a. The maximum R_{hub} in Degree Preserving (denoted by the violet line) is 0.136, which is smaller than that in BP Preserving (denoted by the green line). Therefore, BP Preserving increases $|FVS|$ more than other methods of Degree and SP Preserving and improves R_{hub} to almost the same level as the conventional best in Preserving. Enhancing the loop effectively improves the robustness.

Next, we show the results in BP Non-preserving. At the right in Fig. 3d, BP Non-preserving (denoted by the green line) increases to the maximum $|FVS| = 1549$, which is 53% of nodes are included in FVS. It is about twice larger than $|FVS| = 698$ for the baseline (denoted by the red dot line) at the right in Fig. 3d. In addition, other rewirings in Non-preserving also increase $|FVS|$ at the same level as BP Non-preserving. The maximum $|FVS|$ is 1566 in Degree Non-preserving (denoted by the violet line) and 1527 in SP Non-preserving (denoted by the light blue line) at the right in Fig. 3d. At the right in Fig. 3b, BP Non-preserving (denoted by the green line) increases to the maximum $R_{\text{hub}} = 0.404$. It is also about twice larger than $R_{\text{hub}} = 0.174$ for the baseline (denoted by the red dot line). As similar to the result for $|FVS|$, other methods also increase R_{hub} to almost the same level as BP Non-preserving. The maximum R_{hub} is 0.405 in Degree Non-preserving (denoted by the violet line) and 0.392 in SP Non-preserving (denoted by the light blue line) at the right in Fig. 3b. Therefore, in comparison with the baseline, BP Non-preserving is more effective for improving both R_{hub} and $|FVS|$. Moreover, from the difference between the results in Non-preserving and Preserving, it suggests that modification of the degree distribution significantly affects both R_{hub} and $|FVS|$.

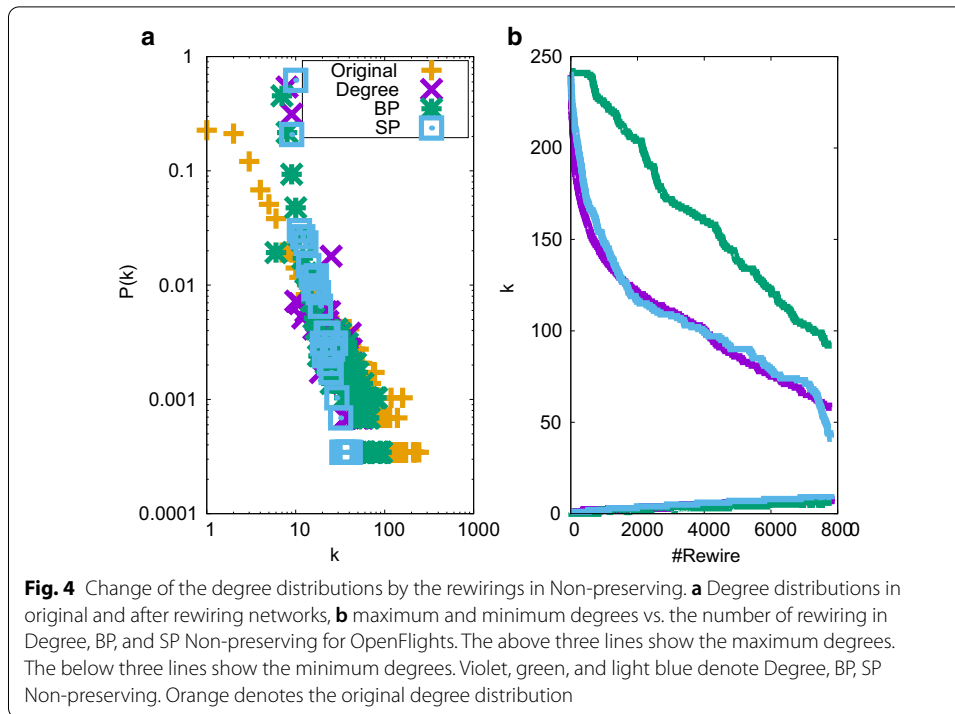
Table 1 The correlation coefficient between R_{hub} and r , and R_{hub} and $|FVS|$ after rewiring

	R_{hub} and r	R_{hub} and $ FVS $
Preserving	0.762	0.970
Non-preserving	0.527	0.980



We find that the rewirings in Non-preserving commonly make the network more homogeneous and reduce the fraction of the high degree nodes as follows. Figure 4a shows the initial degree distribution for OpenFlights and the modified degree distribution after rewired 7800 times by each method. The initial distribution has a long-tailed distribution characterized as a scale-free property, in which the minimum and maximum degrees are 1 and 242. After rewiring by the three methods, a gap between the minimum and maximum degree becomes smaller. In particular, SP Non-preserving modifies to the very narrow gap with the minimum and maximum degree of 9 and 41 in which the 61% occupy the nodes with degree 10. Figure 4b shows that the maximum degree is lower than 100. The methods of Degree, BP, and SP Non-preserving also decrease the gap between the minimum and maximum degrees. Thus, it is suggest that reducing the gap of degrees leads to improve both R_{hub} and $|FVS|$ significantly.

The increases in R_{hub} and $|FVS|$ by BP Non-preserving are partly due to changing the degree distributions as reducing large degree nodes. On the other hand, the increases in them by BP Preserving are only due to enhancing loops with preserving



degrees. However, the values of R_{hub} and $|FVS|$ in BP Non-preserving are larger than ones in BP Preserving.

Relation between the robustness and the size of FVS

In more detailed comparisons, we discuss a relation between R_{hub} and $|FVS|$ in Preserving and Non-preserving. At the left in Fig. 3a, c, e for Preserving, we compare the ordering of BP, Degree, SP Preserving, and WuHolme by the maximum value of each index. It is BP > WuHolme > Degree > SP for R_{hub} , BP > Degree > WuHolme > SP for $|FVS|$, and Degree > BP > WuHolme > SP for r . The order for R_{hub} and $|FVS|$ are almost the same, only the order of Degree and WuHolme are exchanged. As shown in Table 1, R_{hub} and $|FVS|$ have a very strong correlation coefficient of 0.970 in Preserving. On the other hand, the correlation coefficient between R_{hub} and r is 0.762. It is lower than that of R_{hub} and $|FVS|$. These values suggest that $|FVS|$ is more strongly related to R_{hub} than r .

The difference in the ordering is more remarkable in Non-preserving. At the right in Fig. 3b, d, f for Non-preserving, in BP, Degree, SP Non-preserving and WuHolme, it is Degree > BP > SP > WuHolme for both R_{hub} and $|FVS|$, while Degree > BP > WuHolme > SP for r . Furthermore, as shown in Table 1, the correlation coefficient in Non-preserving is 0.980 for R_{hub} and $|FVS|$. It is slightly larger than that in Preserving. On the other hand, the correlation between R_{hub} and r is 0.527, which is smaller than that in Preserving. From these results, the correlation between R_{hub} and r in Non-preserving becomes weaker than that in Preserving. Thus, $|FVS|$ is more strongly related to R_{hub} than r .

Strongly robust networks with negative degree–degree correlations

As known in the onion-like structure, it has been considered that networks with the moderate degree–degree correlations tend to be more robust (Schneider et al. 2011; Tanizawa et al. 2012). However, from the obtained results, we find that networks with the negative degree–degree correlations are possible to be highly robust. Figure 3b, f show that SP Non-preserving (denoted by the light blue line) decreases r , while increases R_{hub} . SP Non-preserving modifies it negatively up to -0.187, showing as the light blue line at the right in Fig. 3f. However, at the right in Fig. 3b, SP Non-preserving increases R_{hub} at the almost same level as both Degree and BP Non-preserving. Note that both Degree and BP Non-preserving make the degree–degree correlations positive over the baseline. These obtained results are commonly found for other networks (See Additional file 1).

Summary

This study proposes a strategy for enhancing loops in increasing the size of FVS to improve the robustness of connectivity. We consider two kinds of rewirings for enhancing loops as BP Preserving and BP Non-preserving. The rewiring in Preserving does not change each node's degree, while the rewiring in Non-preserving changes the degree. We obtain similar results in applying our proposed and conventional rewirings to several real networks (See Additional file 1). From the results, BP Preserving increases the size of FVS effectively. It also improves the robustness index to the level as the same or more than the conventional best. Thus, enhancing loops is a useful strategy for improving robustness. On the other hand, BP Non-preserving increases the robustness index and the size of FVS much more than the conventional best in Preserving. Moreover, the other rewirings in Non-preserving also increase them as the same, and commonly reduce the gap of maximum and minimum degrees. Therefore, it is suggested that reducing the difference in degrees strongly affects increasing the robustness index and the size of FVS. Note that the results in BP Non-preserving are partly due to changing the degree distributions, while ones in BP Preserving are only due to enhancing loops.

In addition, we discuss the relation between the robustness and the size of FVS. The size of FVS is more strongly related to the robustness than the degree–degree correlations in both Preserving and Non-preserving. We also find that existing of strongly robust networks with the negative degree–degree correlations is possible. Therefore, we suggest that enhancing loops is more essential for improvements of robustness than the degree–degree correlations.

Supplementary information

The online version contains supplementary material available at <https://doi.org/10.1007/s41109-020-00343-6>.

Additional file 1: Lists of results for several real networks. This appendix shows the robustness, the size of FVS, and the degree–degree correlations versus the number of rewiring, and change of the degree distributions, as Figs. 3, 4.

Abbreviations

LCCs: Low cost carriers; FSCs: Full service carriers; FVS: Feedback vertex set; BP: Belief propagation; #Rewire: The number of rewiring.

Acknowledgements

Not applicable.

Authors' contributions

YH and MC designed research. MC performed research. MC and YH contributed to develop new methods, analyze data, and wrote the paper. All authors read and approved the final manuscript.

Funding

This research is supported in part by JSPS KAKENHI Grant Number JP.17H01729.

Availability of data and materials

The OpenFlights data that support the findings of this study are available from KONECT—the Koblenz Network Collection, <http://konect.cc/networks/opsahl-openflights/> (Kunegis 2013).

Competing interests

The authors declare that they have no competing interests.

Received: 28 August 2020 Accepted: 8 December 2020

Published online: 09 January 2021

References

- Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. *Phys Rev E* 69(2):025103
- Albert R, Jeong H, Barabási AL (2000) Error and attack tolerance of complex networks. *Nature* 406(6794):378–382
- Barabási AL, Albert R (1999) Emergence of scaling in random networks. *Science* 286(5439):509–512
- Bollobás B (2013) *Modern graph theory*, vol 184. Springer, New York
- Braunstein A, Dall'Asta L, Semerjian G, Zdeborová L (2016) Network dismantling. *Proc Natl Acad Sci* 113(44):12368–12373
- Brooker P (2010) Fear in a handful of dust: aviation and the Icelandic volcano. *Significance* 7(3):112–115
- Buekenhout F, Parker M (1998) The number of nets of the regular convex polytopes in dimension < 4 . *Discrete Math* 186(1):69–94. [https://doi.org/10.1016/S0012-365X\(97\)00225-2](https://doi.org/10.1016/S0012-365X(97)00225-2)
- Chan H, Akoglu L (2016) Optimizing network robustness by edge rewiring: a general framework. *Data Min Knowl Discov* 30(5):1395–1425
- Chang SE, McDaniels TL, Mikawoz J, Peterson K (2007) Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 ice storm. *Nat Hazards* 41(2):337–358
- Chen J, Chen L, Chen Y, Zhao M, Yu S, Xuan Q, Yang X (2019) GA-based Q-attack on community detection. *IEEE Trans Comput Soc Syst* 6(3):491–503. <https://doi.org/10.1109/TCSS.2019.2912801>
- Cohen R, Erez K, Ben-Avraham D, Havlin S (2001) Breakdown of the internet under intentional attack. *Phys Rev Lett* 86(16):3682
- Hayashi Y (2018) A new design principle of robust onion-like networks self-organized in growth. *Netw Sci* 6(1):54–70
- Hayashi Y, Uchiyama N (2018) Onion-like networks are both robust and resilient. *Sci Rep* 8(1):1–13
- Kunegis J (2013) Konec: the koblenz network collection. In: *Proceedings of the 22nd international conference on world wide web*, Association for Computing Machinery, New York, NY, WWW'13 Companion, pp 1343–1350. <https://doi.org/10.1145/2487788.2488173>
- Lipton E (2013) Cost of storm-debris removal in city is at least twice the us average. *The New York Times* <https://www.nytimes.com/2013/04/25/nyregion/debris-removal-from-hurricane-sandy-is-more-costly-than-average.html>. Accessed 26 Aug 2020
- Lordan O, Sallan JM, Escorihuela N, Gonzalez-Prieto D (2016) Robustness of airline route networks. *Phys A Stat Mech Appl* 445(1):18–26
- Lordan O, Sallan JM, Simo P, Gonzalez-Prieto D (2014) Robustness of the air transport network. *Transp Res Part E Logist Transp Rev* 68(1):155–163
- MacKenzie CA, Santos JR, Barker K (2012) Measuring changes in international production from a disruption: case study of the Japanese earthquake and tsunami. *Int J Prod Econ* 138(2):293–302
- Manuel J (2013) The long road to recovery: environmental health impacts of hurricane sandy. *Environ Health Perspect* 121(5):a152–a159
- Minkel JR (2008) The 2003 northeast blackout—five years later. *Scientific American*. <https://www.scientificamerican.com/article/2003-blackout-five-years-later/>. Accessed 26 Aug 2020
- Mugisha S, Zhou HJ (2016) Identifying optimal targets of network attack by belief propagation. *Phys Rev E* 94(1):012305
- Murakami M, Ishikura S, Kominami D, Shimokawa T, Murata M (2017) Robustness and efficiency in interconnected networks with changes in network assortativity. *Appl Netw Sci* 2(1):6
- Newman ME (2002) Assortative mixing in networks. *Phys Rev Lett* 89(20):208701
- Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ (2011) Mitigation of malicious attacks on networks. *Proc Natl Acad Sci* 108(10):3838–3841
- Sun DJ, Zhao Y, Lu QC (2015) Vulnerability analysis of urban rail transit networks: a case study of Shanghai, China. *Sustainability* 7(6):6919–6936
- Tanizawa T, Havlin S, Stanley HE (2012) Robustness of onionlike correlated networks against targeted attacks. *Phys Rev E* 85(4):046109
- Wu ZX, Holme P (2011) Onion structure and network robustness. *Phys Rev E* 84(2):026106
- Xulvi-Brunet R, Sokolov IM (2002) Evolving networks with disadvantaged long-range connections. *Phys Rev E* 66(2):026118

- Yu S, Zhao M, Fu C, Zheng J, Huang H, Shu X, Xuan Q, Chen G (2019) Target defense against link-prediction-based attacks via evolutionary perturbations. *IEEE Trans Knowl Data Eng.* <https://doi.org/10.1109/TKDE.2019.2933833>
- Zhou HJ (2013) Spin glass approach to the feedback vertex set problem. *Eur Phys J B* 86(11):455
- Zhou M, Liu J (2016) A two-phase multiobjective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks. *IEEE Trans Cybern* 47(2):539–552

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► [springeropen.com](https://www.springeropen.com)
