More Tolerant Reconstructed Networks Using Self-Healing against Attacks in Saving Resource

Yukio Hayashi [1,*] **, Atsushi Tanaka** [2] **and Jun Matsukubo** [3]

1   Graduate School of Advanced Science and Technology/Division of Transdisciplinary Sciences, Japan Advanced Institute of Science and Technology, Nomi 923-1292, Japan
2   Graduate School of Science and Engineering, Yamagata University, Yonezawa 992-8510, Japan; tanaka@yamagata-u.ac.jp
3   Department of Creative Engineering, National Institute of Technology Kitakyushu College, Kitakyushu 802-0985, Japan; jmatsu@apps.kct.ac.jp
*   Correspondence: yhayashi@jaist.ac.jp

Abstract: Complex network infrastructure systems for power supply, communication, and transportation support our economic and social activities; however, they are extremely vulnerable to frequently increasing large disasters or attacks. Thus, the reconstruction of a damaged network is more advisable than an empirically performed recovery of the original vulnerable one. To reconstruct a sustainable network, we focus on enhancing loops so that they are not trees, which is made possible by node removal. Although this optimization corresponds with an intractable combinatorial problem, we propose self-healing methods based on enhancing loops when applying an approximate calculation inspired by statistical physics. We show that both higher robustness and efficiency are obtained in our proposed methods by saving the resources of links and ports when compared to ones in conventional healing methods. Moreover, the reconstructed network can become more tolerant than the original when some damaged links are reusable or compensated for as an investment of resource. These results present the potential of network reconstruction using self-healing with adaptive capacity in terms of resilience.

1. Introduction

Unfortunately, the frequency of large disasters or malicious attacks is increasing day by day due to climate change, crustal movements, military conflicts, cyber-terrorism, and mega-urbanization. For example, it is well known that a small accident involved a large-area power collapse in North America [1] and the Italian peninsula [2] in 2003, and that an enormous destruction of social infrastructure systems was caused by the great earthquake in Japan in 2011 [3]. There exists a surprisingly common topological structure called scale-free (SF) in many real networks [4], such as power-grids, airlines, communication, transportation systems, and so on, which support social activities, the economy, industrial production, etc. The SF structure is considered to be generated by a selfish rule—preferential attachment [5]—and consists of many low-degree nodes and a few (high-degree) hubs, heterogeneously. Here, degree means the number of links at a node. Moreover, because of the heterogeneity, a SF network has extreme vulnerability against hub attacks [6]. These vulnerable infrastructures appear everywhere and are interdependent on each other. Since a node prefers to connect high-degree nodes in the efficiency bias to shorten the number of path lengths, counted in hops, preferential attachment encourages the heavy concentration of links to hubs. In many real networks, once hubs are damaged and removed due to malfunction, the remaining nodes are fragmented, and lose their basic

function for, e.g., communication or transportation. It is a plausible scenario for network infrastructures that the weak points of hubs are involved in large disasters.

Therefore, when large-scale failures or attacks occur, the recovery of the original vulnerable network is inadvisable. Instead, reconstruction by healing is required. By changing the structure instead of recovering the original one, a question arises as to how a sustainable network should be reconstructed to maintain the network function. However, because the linking resources (wire cables, wireless communication, or transportation lines between two nodes, etc.) and ports (channels or plug sockets at a node, etc.) are usually limited, allocation should be controlled at the same time as the rewiring or making additional investment for healing. Such a reconstruction conforms with the concept of resilience in system engineering or ecology as a new supple approach to sustaining basic objectives and integrity, even when encountering extreme changes in situations or environments (e.g., following disasters or malicious attacks) for technological systems, organizations, or individuals [7–9].

In this paper, through numerical simulation, we study how to reconstruct a sustainable network under limited-resource conditions, and propose effective self-healing methods based on enhancing loops through a local process around damaged parts. In addition, we show a significant improvement from the previous study [10] by reducing the additional ports prepared in advance besides reusable ports. The motivations for enhancing loops are as follows. In percolation analysis, as a part of network science, it has been found that onion-like structures with positive degree–degree correlations give optimal robustness of connectivity even for a SF network with a power-law degree distribution [11,12]. The "onion-like" description comes from it being visualized by correlations when similar degree nodes are set on a concentric circle arranged in decreasing order of degrees from core to periphery. An onion-like structure can be generated by complete rewiring [11,13], enhancing the correlations under a given degree distribution. On the other hand, since dismantling and decycling problems are asymptotically equivalent at infinite graphs in a large class of random networks with light-tailed degree distribution [14], trees remain without loops at the critical state before complete fragmentation by node removals. The dismantling (or decycling) problem known as NP-hard [15] is aimed at finding the minimum set of nodes for which removal leaves a graph broken into connected components and whose maximum size is at most a constant (or a graph without loops). It is suggested from the equivalence that robustness becomes stronger when as many loops exist as possible. In fact, to be the optimal onion-like network at the same level as the rewired ones [13], enhancing loops by copying [16] or intermediation [17,18] is effective for improving robustness in incrementally growing methods based on a local distributed process such as self-organization. A similar effect is also obtained by preserving or non-preserving the degrees of the nodes after another rewiring based on enhancing loops instead of correlations [19]. Thus, we remark that loops make bypasses, and may be more important than degree–degree correlations improving the connectivity in a network reconstruction after a large disaster or attack. This is predicted to be the top priority for maximizing the decycling set (called the Feedback Vertex Set (FVS) in computer science [15]) so as not to create trees without loops as much as possible even in the worst case of node removal. In other words, enhancing loops corresponds to the optimizing of the tolerance of connectivity in graphs (but not in the context of general computing or problem-solving). Of course, increasing the path lengths between nodes and wasteful resources should be avoided during reconstruction by healing. However, even the identification of the necessary nodes to form loops is intractable due to combinatorial NP-hardness [15]. We effectively apply an approximate calculation by Belief Propagation (BP) based on a statistical physics approach in our self-healing through rewiring (or additional investment), which will be mentioned later. We describe the healing methods as sequential processes for computer simulation, envisioning the further development of distributed control algorithms.

2. Methods

2.1. Outline of Healing Process

Almost simultaneously attacked nodes are not recoverable immediately. Therefore, they are removed from network function for an amount of time. In such a case of emergency for healing, two unconnected nodes are chosen and rewired, as the reconstruction assistance or reuse of links emanates from the removal of qN nodes, when the fraction of attacks is q and N denotes the total number of nodes (as the network size). Some of disconnected links may be reusable on neighboring sides depending on the damage level. Although we call the reuse "rewiring", removal of nodes is a different problem to that in the so-called "usual" rewiring methods [11,13,19]. The outline of the healing process is as follows.

Step 0: Detection and initiation

After detecting a removal as a malfunction at the nearest neighbor of the attacked node, the healing process is initiated autonomously.

Step 1: Selection of two nodes

Since the neighbor loses links at least temporarily before rewiring, the damaged ones become an attached candidate for healing. Thus, two unconnected nodes are chosen from the neighbors of the nodes removed by attacks. The selections are different in our proposed and the conventional healing methods. Moreover, neighbors are extended in our proposed methods.

Step 2: Rewiring for healing

The chosen two nodes are connected as rewiring for healing. The above process is repeated for $M_h \stackrel{\text{def}}{=} r_h \times \tilde{\sum}_{i \in D_q} k_i$ links.

Here, $\tilde{\sum}_{i \in D_q} k_i$ means the number of disconnected links by attacks without multiple counts. D_q denotes the set of removed nodes, $|D_q| = qN$. M_h includes the number of reused and additionally invested links. When reusable links are insufficient, we assume the addition of links as an investment in the considered M_h for a parameter $0 < r_h \leq 1$ in computer simulation.

In the healing process, rewirings are performed by changing directions and ranges of flight routes or wireless beams. However, we will not discuss the details of realization, which depends on current or future technologies and target systems. Here, we focus on connectivity at the most fundamental level in many network systems for not only communication but also transportation, power supply, and other infrastructures, while our approach may be useful for path control or failure detection, e.g., by software-defined network-based reconfiguration of communication systems with switches in managing reliability, latency, or security at some service levels [20–22]. In addition, we consider that ports work independently from links, similar to the relationship between an airport runaway or plug socket and an airplane flight or cable line. It is a reasonable assumption that the amount of degree k_j ports is reusable at the undamaged neighbor node $j \in \partial i$ of a removed node i by attacks, where ∂i denotes a set of the nearest connecting neighbors of i. Thus, there exist at least as many active (reusable) ports of a node as its degree in the original network before any attacks.

2.2. Proposed Healing Methods

In our proposed healing methods, there are two phases: ring formation and enhancing loops by applying BP in the next subsection. Moreover, they (RingRecal, RingLimit1,5,10, RingLimit5Recal) are modified to reduce the additional ports from the previous results [10] by avoiding the concentration of links at some nodes.

RingBP Previously, our combination method of ring formation and enhancing loops was based on [10]. After making rings on the extended neighbors of removed nodes, as shown in Figure 1, enhancing the loops on the rings is performed by applying the BP algorithm [23] (see Section 2.3). However, in BP, a set $\{p_i^0\}$ as probability of node i to

be necessary for loops is calculated only once, just after an attack. Please note that a ring is the simplest loop when it uses the least number of links.

RingRecal We modified our method with the recalculation of BP. After making rings, a set $\{p_i^0\}$ is recalculated one by one through each rewiring in the remaining links within M_h for enhancing loops.

RingLimit1,5,10 We modified our method with limited rewirings. After making rings, in enhancing loops, the number of rewiring links is limited at node i to its degree k_i +1, +5, or +10.

RingLimit5Recal We modified our method by a combination of RingRecal and RingLimit5. After making rings, a set of $\{p_i^0\}$ is recalculated one by one through each rewiring in the remaining links within M_h for enhancing loops. Moreover, the number of rewiring links is limited at node i to $k_i + 5$.

First, in ring formation (see Figure 1), the order of process is basically according to the order of the removed nodes $i_1, i_2, \ldots, i_{qN}$. Thus, rings are made for the neighbors $\partial i_1, \partial i_2, \ldots, \partial i_{qN}$ in this order. However, if there is $i_{k'} \in \partial i_k$, $k' > k$, it is extended as the union $\partial i_k \leftarrow \partial i_k \cup \partial i_{k'}$. In addition, if there is $i_{k''} \in \partial i_{k'}$, $k'' > k'$, it is also extended as the union $\partial i_k \leftarrow \partial i_k \cup \partial i_{k'} \cup \partial i_{k''}$. Such extensions of neighbors are repeated until a ring encloses the induced subgraph of removed nodes and their links. To make a ring, a node is chosen u.a.r. and connected to a subsequent similarly chosen node in a set of the extended neighbors. This is repeated without multi-selections until a return is made to the first chosen node from the last chosen node.

Next, when enhancing loops on each ring for the remaining rewirings in M_h, a node j with the minimum p_j^0 is chosen in all the neighbors of the removed nodes, and connected to the other node j' with the second minimum $p_{j'}^0$ on the ring to which j belongs. For each rewiring, a set of $\{p_i^0\}$ is recalculated one by one in RingRecal and RingLimit5Recal methods. In addition, the number of rewiring links is limited at node i to $k_i + 5$ (or $+1$, $+10$) according to its degree k_i in RingLimit5Recal and RingLimit5 (or RingLimit1, RingLimit10) methods. If the condition is unsatisfied, another node with a second, third, fourth, and subsequent minimum is chosen as a candidate for healing. Although a node j'' with small $p_{j''}^0$ tends not to contribute to making loops because it is not included in FVS, it is expected that the number of loops is increased by connecting such nodes. This is the reason for the above selection.
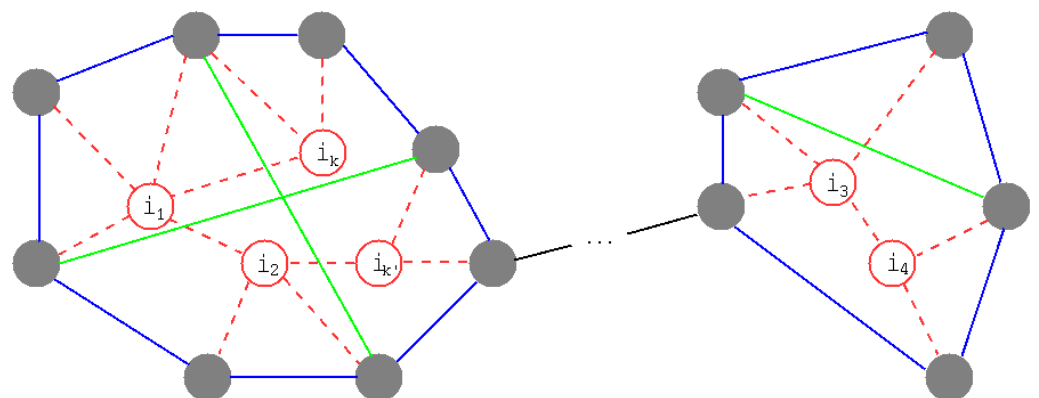

Figure 1. Schematic illustration of ring formation and enhancing loops. Red nodes and their links are removed by attacks. Gray filled nodes are the neighbors. Blue lines make rings, and green lines are rewirings for enhancing loops on rings.

2.3. Applying the Belief Propagation Algorithm

To calculate the probability p_i^0 of belonging to FVS, the following BP algorithm [23] is applied. It is based on a cavity method in statistical physics. We review the outline derived for approximately estimating FVS known as the NP-hard problem [15]. In the

cavity graph, it is assumed that nodes $j \in \partial i$ are mutually independent of each other when node i is removed (the exception is denoted by $\backslash i$). Then the joint probability is $\mathcal{P}_{\backslash i}(A_j : j \in \partial i) \approx \Pi_{j \in \partial i} p_{j \to i}^{A_j}$ by the product of independent marginal probability $p_{j \to i}^{A_j}$ for the state A_j as the node index of j's root or empty 0: it belongs to FVS. The corresponding probabilities are represented by

$$p_i^0 \overset{\text{def}}{=} \frac{1}{z_i(t)}, \tag{1}$$

$$p_{i \to j}^0 = \frac{1}{z_{i \to j}(t)}, \tag{2}$$

$$p_{i \to j}^i = \frac{e^x \Pi_{k \in \partial i(t) \backslash j} \left[p_{k \to i}^0 + p_{k \to i}^k \right]}{z_{i \to j}(t)}, \tag{3}$$

where $\partial i(t)$ denotes node i's set of connecting neighbor nodes at time t, and $x > 0$ is a parameter of inverse temperature. The normalization constants are

$$z_i(t) \overset{\text{def}}{=} 1 + e^x \left[1 + \sum_{k \in \partial i(t)} \frac{1 - p_{k \to i}^0}{p_{k \to i}^0 + p_{k \to i}^k} \right] \Pi_{j \in \partial i(t)} \left[p_{j \to i}^0 + p_{j \to i}^j \right], \tag{4}$$

$$z_{i \to j}(t) \overset{\text{def}}{=} 1 + e^x \Pi_{k \in \partial i(t) \backslash j} \left[p_{k \to i}^0 + p_{k \to i}^k \right] \times \left[1 + \sum_{l \in \partial i(t) \backslash j} \frac{1 - p_{l \to i}^0}{p_{l \to i}^0 + p_{l \to i}^l} \right], \tag{5}$$

to be satisfied for any node i and link $i \to j$ as

$$p_i^0 + p_i^i + \sum_{k \in \partial i} p_i^k = 1, \quad p_{i \to j}^0 + p_{i \to j}^i + \sum_{k \in \partial i} p_{i \to j}^k = 1.$$

We repeat these calculations of message-passing until they are self-consistent in principle but practically reach appropriate rounds from an initial setting of $(0, 1)$ random values. The unit time from t to $t + 1$ for calculating a set $\{p_i^0\}$ consists of several rounds by updating Equations (1)–(5) in order of random permutation of the total N nodes. Since the sums or products in Equations (1)–(5) are restricted in the nearest neighbor, they are local processes. The distributed calculations can be also considered. As included in FVS, a node k with the maximum p_k^0 is chosen. After removing the chosen node, $\{p_i^0\}$ is recalculated the next time. Such a process is repeated until it is acyclic for finding the FVS. However, in our healing method, $\{p_i^0\}$ is used to select the attached two nodes on a ring by rewiring.

2.4. Conventional Healing Methods

We briefly explain the following typical healing methods in network science (inspired by fractal statistical physics) and computer science.

RBR Conventional Random Bypass Rewiring (RBR) method [24] (corresponds to $r_h = 0.5$).

GBR Greedy Bypass Rewiring (GBR) method improved from RBR heuristically [24].

SLR Conventional Simple Local Repair (SLR) method [25] with priority of rewirings to more damaged nodes.

In network science, a self-healing method that adds new random links to interdependent two-layered networks of square lattices has been proposed, and the effect against node attacks is numerically studied [26]. In particular, for the addition of links by the healing process, the candidates of linked nodes are incrementally extended from only the direct (nearest connecting) neighbors of the removed node by attacks until no more separation of components occurs. In other words, connectivity is maintained except for the isolating removed parts. Such extension of the candidates of linked nodes is a key idea in our proposed self-healing method.

Furthermore, the following self-healing methods, whose effects are investigated for some data of real networks, are worthy to note. One is a distributed SLR [25] with repair by a link between the most damaged node and a randomly chosen node from the unremoved node set in its next-nearest neighbor before attacks. The priority of the damaged nodes is according to the smaller fraction k_{dam}/k_{orig} of its remained degree k_{dam} and the original degree k_{orig} before the attacks. The selections are repeated until reaching a given rate f_s controlled by the fraction of nodes whose k_{dam}/k_{orig} falls below a threshold. Another is RBR [24] on the more limited resources of links and ports. To establish links between pair nodes, a node is randomly chosen only one time from the neighbors of each removed node. When k_i denotes the degree of the removed node i, only $\lfloor k_i/2 \rfloor$ links are reused. Please note that reserved additional ports are not necessary: they do not exceed the original one before attacks. Moreover, GBR [24] is proposed to improve the robustness; the selection of pair nodes is based on the number of the links not yet rewired and the size of the neighboring components.

In computer science, the ForgivingTree algorithm has been proposed [27]. Under repeated attacks, the following self-healing is processed one by one after each node removal, except when the removed node is a leaf (whose degree is one). This is based on both a distributed process of sending messages and data structure, further developed to an efficient algorithm called compact routing [28]. In each rewiring process, a removed node and its links are replaced by a binary tree. Please note that each vertex of the binary tree was the neighbors of the removed node, whose links to the neighbors are reused as the edges of the binary tree. Thus, additional links for healing are unnecessary, but not controllable. It is remarkable for computation (e.g., in routing or information spreading) that the multiplicative factor of the diameter of the graph after healing is never more than $O(\log k_{max})$, where k_{max} is the maximum degree in the original network because of the replacement by binary trees. However, the robustness of connectivity is not taken into account in the limited rewiring based on binary trees, since a tree structure is easily fragmented into subtrees by any attack on the articulation node. Thus, this healing method is excluded from compared ones.

3. Results

We evaluate the effect of healing by four measures: the ratio $S(q)/N_q$ [25] for the connectivity, the robustness index $R(q) \stackrel{\text{def}}{=} \sum_{q'} S_q(q')/N_q$, the efficiency of paths $E(q) \stackrel{\text{def}}{=} \frac{1}{N_q(N_q-1)} \sum_{i \neq j} \frac{1}{L_{ij}}$, and the average degree $k_{avg}(q)$ in $N_q \stackrel{\text{def}}{=} (1-q)N$ nodes, where $S(q)$ and $S_q(q')$ denote the sizes of GC (giant component or largest connected cluster) after removing qN nodes by attacks from the original network and removing $q'N_q$ nodes by further attacks from the surviving N_q nodes, respectively. Here, a removed node is chosen with recalculation of the highest degree node as the target. Remember that $q = 1/N, 2/N, \ldots, (N-1)/N$ (or $q' = 1/N_q, 2/N_q, \ldots, (N_q-1)/N_q$) is a fraction of attacks. Although $S(q)$ or $S_q(q')$ represents the size of GC after attacks to qN or $q'N_q$ nodes, $R(q)$ is a measure of tolerance of connectivity against further attacks. L_{ij} denotes the length of the shortest path counted by hops between i-j nodes in the surviving N_q nodes. The ranges are $0 < S(q)/N_q \leq 1$, $0 < R(q) \leq 0.5$, and $0 < E(q) \leq 1$. We investigate the four measures before or after healing for OpenFlights between airports, Internet AS Oregon, and US PowerGrid as examples of typical infrastructures of SF networks [29–31] after extracting from each of them to a connected and undirected graph without multiple links (see Table 1). We compare the results shown by color lines with marks in figures for the conventional RBR, GBR, SLR, and our proposed RingBP, RingRecal, RingLimit1,5,10, RingLimit5Recal methods.

In each of Figures 2–5, no-healing, conventional, and previous our methods are compared in (a), previous our and RingRecal or RingLimit methods are compared in (c,d), previous our and the best combination RingLimit5Recal methods are compared in (b). Red, green, blue, orange, and purple lines denote the rate $r_h = 0.05, 0.1, 0.2, 0.5$ and 1.0, respectively, for the number M_h of rewirings. The results for the original and no-healing

networks are shown by dashed magenta and solid black lines. The following results are averaged over 100 samples with random process for tie-breaking in a node selection or ordering of nodes on a ring.

Table 1. Basic properties for the original networks. N and M denote the numbers of nodes and links. $k_{avg} = 2M/N$, k_{min}, and k_{max} are the average, minimum, and maximum degrees. L_{avg}, D, R and E denote the average path length, diameter, robustness index, and efficiency of paths, respectively.

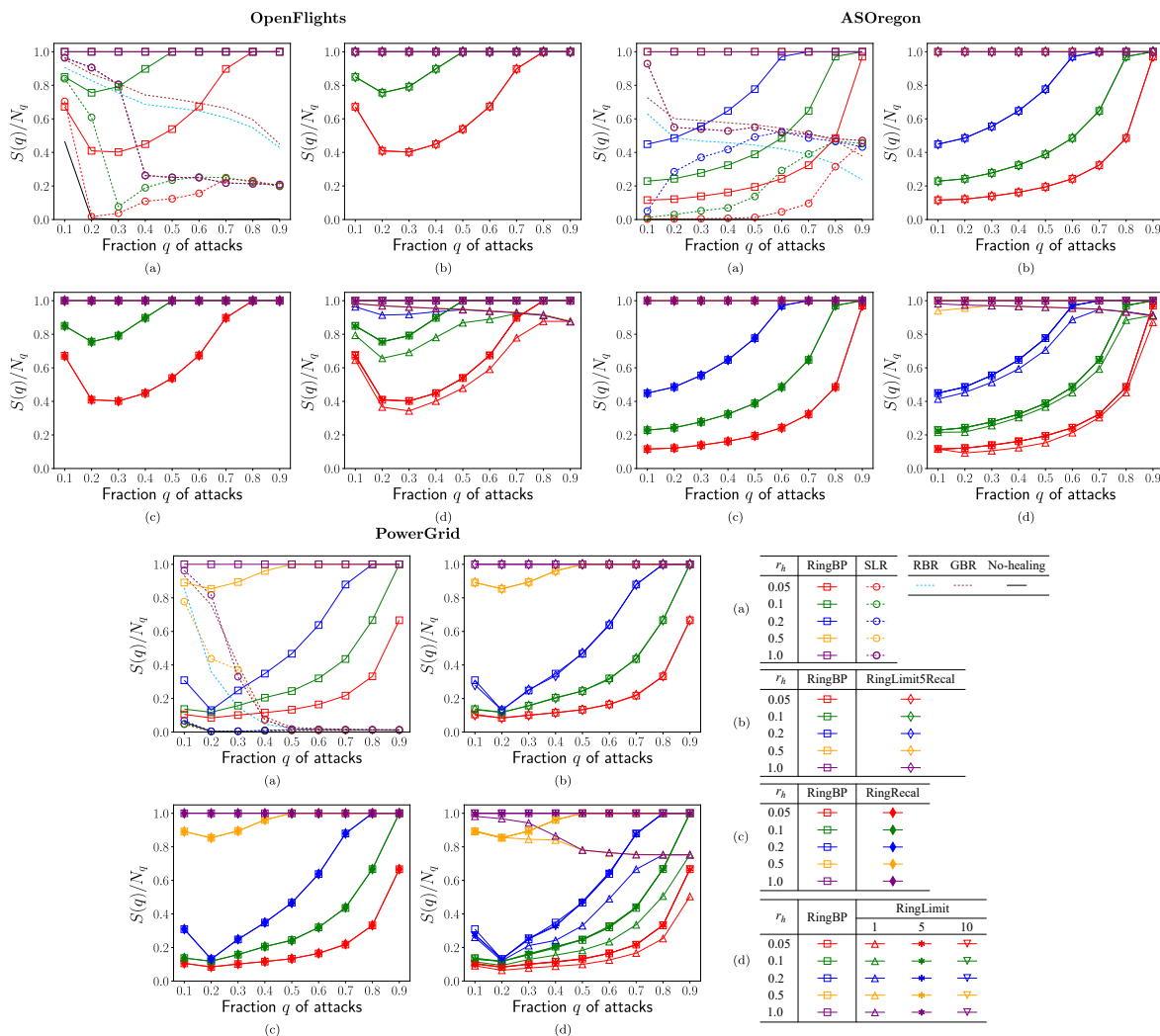| Network	N	M	k_{avg}	k_{min}	k_{max}	L_{avg}	D	R	E
OpenFlight	2905	15,645	10.77	1	242	4.097	14	0.080912	0.266934
AS Oregon	6474	12,572	3.883	1	1458	3.705	9	0.012500	0.290399
PowerGrid	4941	6594	2.669	1	19	18.989	46	0.052428	0.062878

Figure 2. Ratio $S(q)/N_q$ of connectivity vs. fraction q of attacks for the rate r_h in rewirings. (**a**) SLR, RBR, GBR, RingBP, (**b**) RingBP, RingLimit5Recal, (**c**) RingBP, RingRecal, and (**d**) RingBP, RingLimit1,5,10 methods.

Figure 2 shows the ratio $S(q)/N_q$ of connectivity in the surviving N_q nodes. Remember that $S(q)$ is the size of GC after healing (or no-healing) against attacks to qN nodes. Higher ratio means larger connectivity, as maintaining the network function for communication or transportation, $S(q)/N_q < 1$ indicates the incomplete ring formation stopped in M_h. As shown in Figure 2a, the ratio rapidly decreases in the conventional SLR method marked by open circles for OpenFlights and PowerGrid, while it is moderately higher around $S(q)/N_q \approx 0.5$ on purple and blue lines or increasing in green and red lines marked by open circles for AS Oregon. Moreover, in Figure 2a, the following results are common for

OpenFlights, AS Oregon, and PowerGrid. The ratio also decreases in the conventional RBR and GBR methods denoted by dashed light blue and brown lines, respectively. In the corresponding RingBP method, the ratio is the highest as the horizontal orange (but overlapped purple) line at $S(q)/N_q \approx 1.0$ marked by open squares. The bottom dashed black lines around $S(q)/N_q = 0$ are the results without the network function for no-healing. Thus, previously, our RingBP method marked by open squares had higher ratio than the conventional methods in comparison with the same color lines. Figure 2b,c shows that the ratio in RingBP method marked by open squares almost coincides with the ones in the RingLimit5Recal method marked by open diamonds and RingRecal method marked by filled diamonds. Similarly, Figure 2d shows that the ratio in RingBP method marked by open squares almost coincides with ones in RingLimit5,10 methods marked by lower triangles and asterisks. However, it is slightly lower in the RingLimit1 method marked by open upper triangles. Therefore, RingLimit5Recal, RingRecal, and RingLimit5,10 methods are the best at the same level to RingBP in maintaining connectivity. The constraint to the number of additional ports is slightly too strong as there is only one in the RingLimit1 method.
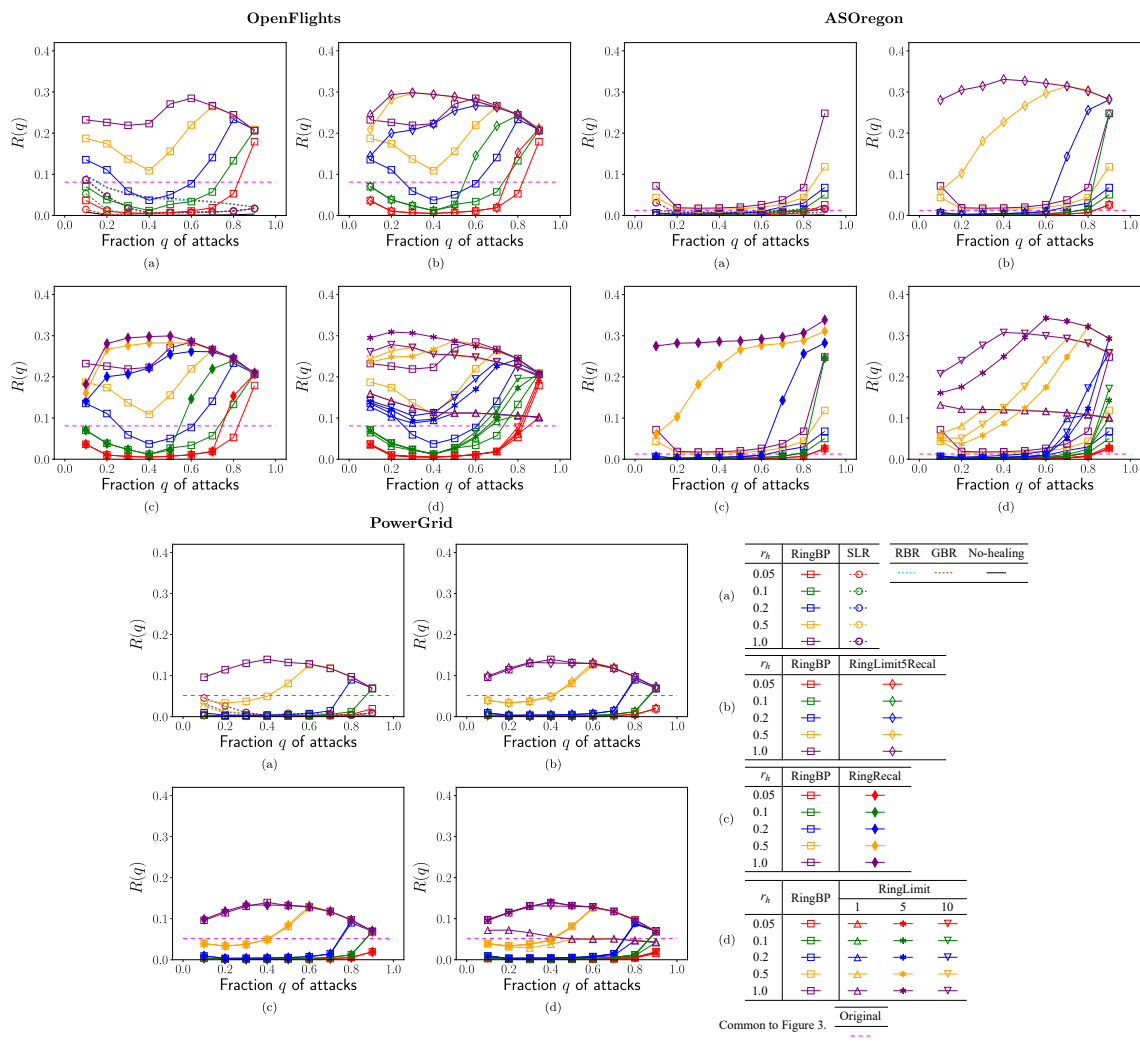

Figure 3. Robustness index as the tolerance of connectivity against further attacks to the surviving N_q nodes vs. fraction q of attacks for the rate r_h in rewirings. (**a**) SLR, RBR, GBR, RingBP, (**b**) RingBP, RingLimit5Recal, (**c**) RingBP, RingRecal, and (**d**) RingBP, RingLimit1,5,10 methods.

Figure 3 shows the robustness index $R(q)$ as the tolerance of connectivity against further attacks to the surviving N_q nodes after healing. Please note that a major part of N_q nodes belong to the GC, but other parts belong to isolated clusters. In Figure 3a for

OpenFlights, AS Oregon, and PowerGrid, the values of $R(q)$ rapidly decrease to very low level ≤ 0.1 with vulnerability in the conventional SLR method marked by open circles and in RBR and GBR methods denoted by light blue and brown dashed lines, while there exist higher values of $R(q)$ (on purple and orange lines for $r_h \geq 0.5$) in RingBP method marked by open squares than the horizontal dashed magenta lines in the original network. The results for no-healing are at the bottom as $R(q) \approx 0$ because of $S_q \approx 0$ from Figure 2a. Moreover, as shown in Figure 3b,c, RingLimit5Racal method marked by open diamonds and RingRecal method marked by filled diamonds have higher values of $R(q)$ than RingBP marked by open squares in comparison with same color lines for OpenFlights and AS Oregon, while these methods have almost same values of $R(q)$ to ones in RingBP for PowerGrid. Similarly, as shown in Figure 3d for OpenFlights and AS Oregon, RingLimit1,5,10 methods marked by open lower, upper triangles, and asterisks have higher values of $R(q)$ than RingBp method marked by open squares in comparison with same color lines. However, the difference becomes smaller in green and red lines for $r_h \leq 0.1$. In Figure 3d for PowerGrid, similar values of $R(q)$ are obtained on each color line regardless of marks for different methods. In particular, for OpenFlights and AS Oregon, purple, orange and blue line ($r_h \geq 0.2$) in RingLimit5Recal marked by open diamonds are slightly higher than ones in Ringlimit1,5,10 marked by open upper, lower triangles and asterisks as shown in Figure 3b,d. Thus, the reconstructed networks by our proposed healing methods can become stronger with higher values of $R(q)$ than the original network against further attacks. In particular, the improvement is remarkable from $R(q) < 0.1$ to $R(q) > 0.3$ for OpenFlights and AS Oregon.
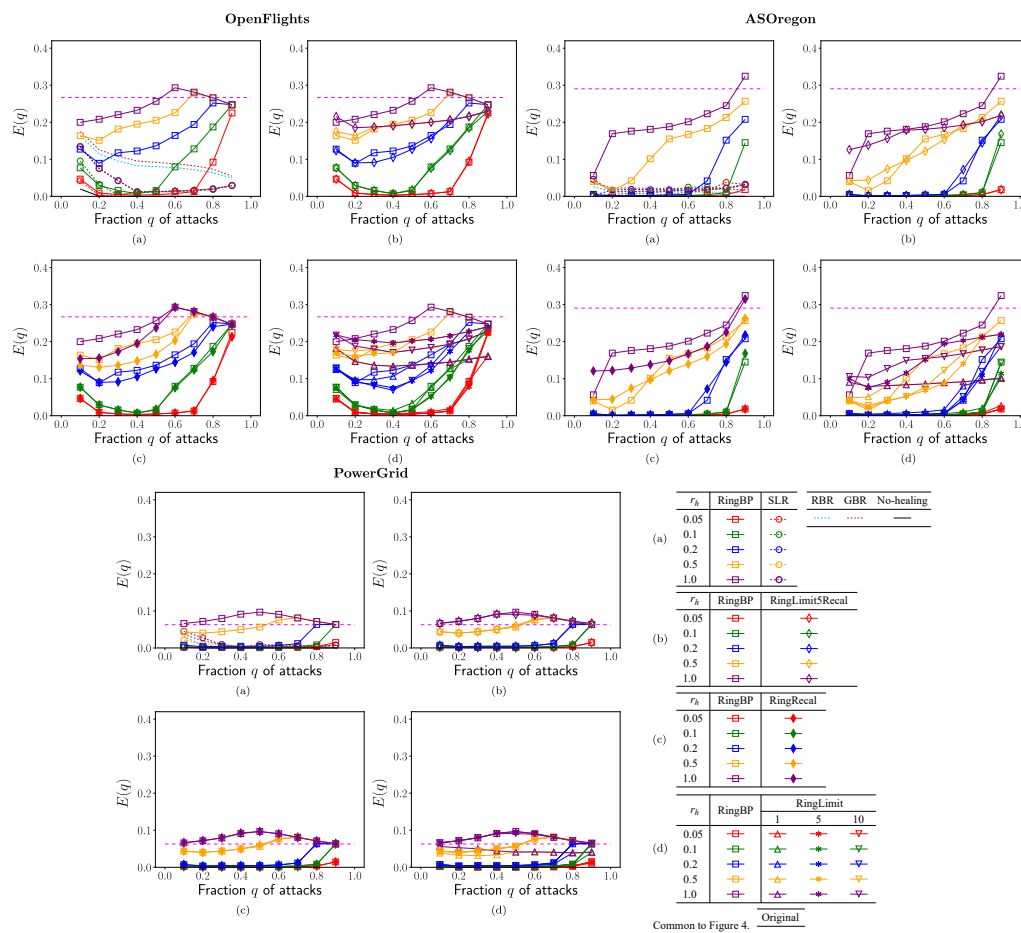

Figure 4. Efficiency of paths in the surviving N_q nodes vs. fraction q of attacks for the rate r_h in rewirings. (**a**) SLR, RBR, GBR, RingBP, (**b**) RingBP, RingLimit5Recal, (**c**) RingBP, RingRecal, and (**d**) RingBP, RingLimit1,5,10 methods.

Figure 4 shows the efficiency $E(q)$ of shortest paths between two nodes in the surviving N_q nodes. Please note that $E(q) = 0.1, 0.2, 0.25$ corresponds to $10, 5, 4$ hops of the average path length $L_{avg}(q)$ from $L_{avg}(q) \approx 1/E(q)$ in the arithmetic and the harmonic means of path lengths. The following results are common for OpenFlights, AS Oregon, and PowerGrid. As with Figures 2a–4a that show that the values of $E(q)$ rapidly decrease in the conventional SLR method marked by open circles, RBR and GBR methods are denoted by light blue and brown dashed lines, while the values are higher in RingBP method are marked by squares in comparison with same color lines. In Figure 4b,c, RingLimit5Recal method marked by open diamonds and RingRecal method marked by filled diamonds have similar or slightly lower values of $E(q)$ than ones in RingBP method marked by squares in comparison with the same color lines. In Figure 4d for OpenFlights and AS Oregon, the values are slightly lower in RingLimit1,3,5 methods marked by open upper triangles, lower triangles, and asterisks than ones in RingBP method marked by squares, while for PowerGrid the values are similar regardless of these methods in comparison with same color lines.
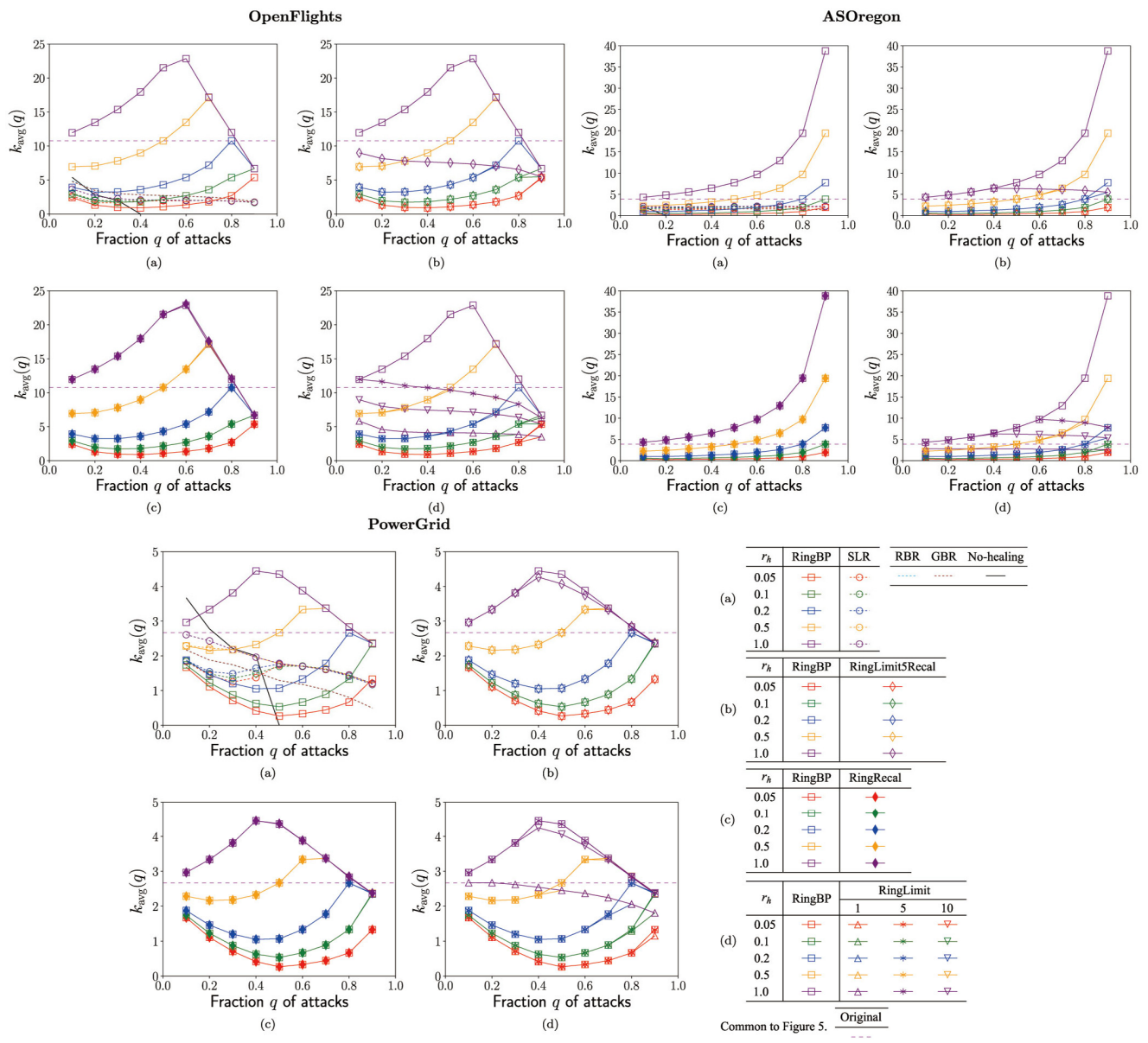

Figure 5. Averagedegree $k_{avg}(q)$ in the surviving N_q nodes vs. fraction q of attacks for the rate r_h in rewirings. (**a**) SLR, RBR, GBR, RingBP, (**b**) RingBP, RingLimit5Recal, (**c**) RingBP, RingRecal, and (**d**) RingBP, RingLimit1,5,10 methods.

Figure 5 shows the average degree $k_{avg}(q)$ in the surviving N_q nodes. This value indicates how much links are effectively used for hearing. In other words, a small value of $k_{avg}(q)$ means that rewirings are restricted and not fully used until the possible number M_h of links, especially in conventional methods, by the constraints on linking between not the extended but the nearest neighbors of attacked nodes or the limitation (see Section 2.4). The following results are common for OpenFlights, AS Oregon, and PowerGrid. As shown in Figure 5a, it is remarkable that the values are small ($k_{avg}(q) < 10$) in the conventional SLR method marked by open circles, and RBR and GBR methods denoted by dashed light blue and brown lines, while the values are higher in RingBP method marked by open squares, in comparison with the same color lines. In Figure 5b,d, by saving rewired links due to the limitation of additional ports, the values of $k_{avg}(q)$ are not large in the RingLimit5Recal method marked by open diamonds or in RingLimit1,5,10 methods marked by open upper triangles, lower triangles and asterisks. In Figure 5c, on each color line, the values of $k_{avg}(q)$ in RingBP method marked by open squares are almost coincident with the ones in the RingRecal method marked by filled diamonds. However, in RingLimit5Recal and RingLimit1,5,10 methods with saving rewired links, both $R(q)$ and $E(q)$ are high values as shown in Figures 3b,d and 4b,d. Therefore, these methods are more effective for healing to improve the robustness and efficiency to similar levels by using less resource. Figure 6 shows that the reconstructed degree distribution $P(k)$ in RingLmit5Recal method becomes exponential approximately in a semi-logarithmic plot from a power-law in the original network. The maximum degrees are bounded as 65, 19, and 14 for OpenFlights, AS Oregon, and PowerGrid, respectively. They tend to be smaller as q increases.
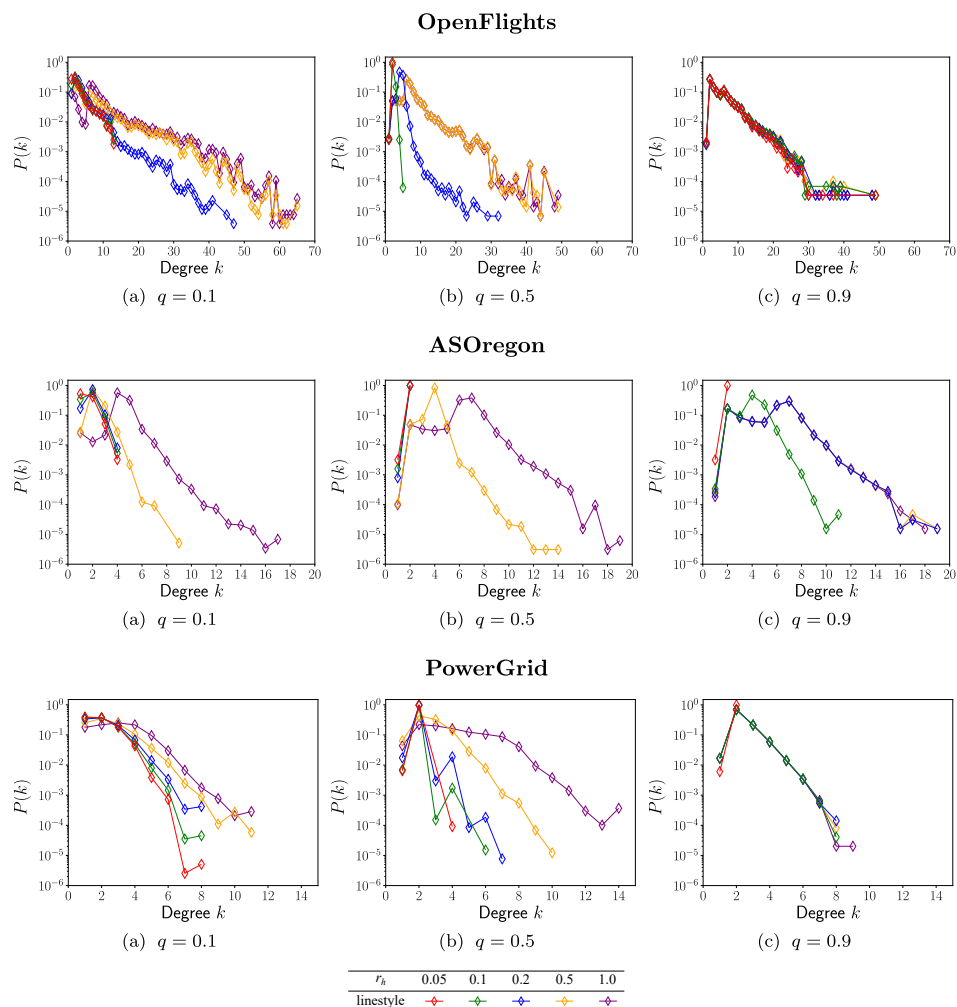

Figure 6. Degree distribution in surviving N_q nodes after healing by RingLimit5Recal method for the fraction of attacks.

Table 2. Maximum number of additional ports (the average number in parenthesis) for the fraction q of attacks and the rate r_h in rewirings.

OpenFlights									
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.05	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	2 (1.36)	14.7 (3.32)
0.1	1 (1)	1 (1)	1 (1)	1 (1)	2 (1.10)	2 (1.37)	4.03 (1.91)	20.68 (3.55)	21.59 (4.46)
0.2	26.54 (1.66)	3.67 (1.59)	3.44 (1.68)	3.81 (1.91)	10.22 (2.51)	29.44 (3.64)	44.08 (5.47)	49.23 (8.46)	21.56 (4.46)
0.3	55.44 (3.57)	23.93 (2.83)	26.55 (3.02)	42.07 (3.72)	50.64 (4.86)	65.58 (6.56)	69.37 (8.92)	63.04 (9.74)	21.61 (4.46)
0.4	77.65 (5.57)	56.61 (4.44)	62.22 (4.81)	69.58 (5.74)	79.96 (7.20)	88.11 (9.28)	81.62 (12.17)	63.09 (9.73)	21.6 (4.46)
0.5	96.35 (7.56)	81.88 (6.07)	87.52 (6.61)	98.26 (7.77)	106.62 (9.59)	105.12 (11.84)	107.14 (14.84)	62.99 (9.74)	21.62 (4.46)
1.0	179.04 (16.78)	175.97 (13.95)	173.53 (14.85)	177.32 (16.91)	160.94 (19.68)	170.93 (20.66)	115.33 (15.10)	63.02 (9.74)	21.57 (4.46)

AS Oregon									
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.05	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)
0.1	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	6.43 (2.26853)
0.2	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)	2.03 (1.29)	6.44 (2.23)	56.47 (6.30)
0.3	1 (1)	1 (1)	1 (1)	1 (1)	2 (1.21)	3.08 (1.42)	6.67 (2.22)	49.06 (4.21)	85.74 (10.38)
0.4	1 (1)	1 (1)	2 (1.16)	2 (1.31)	3.66 (1.57)	5.48 (2.21)	48.89 (3.53)	79.8 (6.24)	107.53 (14.48)
0.5	2.49 (1.11)	2 (1.26)	2 (1.37)	3.77 (1.68)	6.22 (2.22)	48.81 (3.20)	79.89 (4.88)	104.12 (8.25)	127.04 (18.54)
1.0	40.64 (2.67)	73.63 (3.20)	93.29 (3.92)	111.4 (4.87)	128 (6.22)	146.73 (8.21)	164.37 (11.56)	181.31 (18.30)	199.37 (38.81)

PowerGrid									
	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9
0.05	1.08 (1.00)	1 (1)	1.02 (1.00)	1.01 (1.00)	1 (1)	1 (1)	1 (1)	1 (1)	1 (1)
0.1	1.65 (1.01)	1.99 (1.01)	1.93 (1.02)	1.59 (1.00)	1.15 (1.00)	1.02 (1.00)	1.04 (1.00)	1.02 (1.00)	3.81 (1.19)
0.2	2 (1.02)	2.1 (1.02)	2.12 (1.03)	2.25 (1.03)	2.13 (1.02)	1.91 (1.00)	2.01 (1.01)	3.8 (1.32)	3.69 (1.19)
0.3	2 (1.02)	2.59 (1.05)	2.95 (1.07)	2.93 (1.07)	2.95 (1.08)	3.01 (1.10)	3.12 (1.27)	6.21 (1.51)	3.74 (1.19)
0.4	2.42 (1.04)	3.06 (1.09)	3.25 (1.10)	3.14 (1.13)	3.25 (1.15)	3.11 (1.26)	8.99 (1.90)	6.27 (1.51)	3.74 (1.19)
0.5	2.87 (1.06)	3.76 (1.11)	3.47 (1.14)	3.47 (1.17)	3.31 (1.27)	5.66 (1.78)	9.03 (1.90)	6.35 (1.51)	3.77 (1.19)
1.0	4.9 (1.64)	6.08 (1.86)	13.42 (2.31)	15.44 (2.94)	14.95 (2.80)	11.85 (2.35)	9.01 (1.90)	6.29 (1.51)	3.78 (1.19)

Table 2 shows the maximum number (or in parentheses, the average value over the nodes that perform much more rewirings than their degrees of the reusable number of ports) of additional ports in the RingRecal method. Although the values are reduced to less than k_{max} from nearly $2k_{max} \sim 3k_{max}$ in our previous RingBP method [10], they are still large. Here, k_{max} is 242, 1458, or 19 for the original networks OpenFlights, AS Oregon, or PowerGrid are shown in Table 1. Of course, the maximum number of additional ports is significantly restricted to a constant 1, 5, 10 or 5 in RingLimit1,5,10 or RingLimit5Recal method. Since the additional ports should be stored in advance beside a reusable number of its degree in the original network, less preparation is better with a lower investment cost of resource. Thus, RingBP or RingRecal method is not desirable, because it requires many additional ports.

4. Discussion

We have proposed self-healing methods with modifications from the previous one [10] for reconstructing a resilient network through rewirings against attacks or disasters in the resource allocation control of links and ports. The healing strategy is based on maintaining connectivity using ring formation on the extended neighbors of attacked nodes and enhancing loops to improve the robustness of connectivity in applying the approximate calculations of BP [23] inspired by statistical physics in a distributed manner. We have taken into account the limitation of additions and the recalculations of BP as modifications to reduce the preparation of additional ports by avoiding the concentration of links at some nodes.

Simulation results show that our proposed combination methods of ring formation and enhancing loops are better than the conventional SLR [25], RBR, and GBR [24] methods. In particular, in the RingLimit5Recal method, both high robustness of connectivity and efficiency of paths are obtained by saving the resource of links and ports, even though the number of additional ports is significantly restricted to a constant 5 from the previous $O(k_{max}) \sim 10^3$ [10]. Moreover, we have found that the reconstructed networks by healing can become more robust and efficient than the original networks before attacks, when some extent of damaged links are reusable or compensated for as the rate $r_h \geq 0.5$.

However, what structure is the optimally tolerant against further attacks in varying the degree distribution after healing remains an open question. Even if our prediction comes true, it is not yet known what approach is more effective and practical for approximately maximizing the FVS. These challenging problems are beyond the discussion of onion-like structure under a given degree distribution [11,12]. In addition, how the healing method should be extended to interdependent or multilayer networks as networks of networks is an intensive issue. On the other hand, in application points of view, further investigations will be useful for other networks if huge computation is available, since our obtained results seem to depend on special topological structures such as PowerGrid with a large diameter D (see Table 1). The development of distributed algorithms within only local information is also important for our self-healing methods.

Author Contributions: Conceptualization, Y.H.; methodology, Y.H.; software, A.T. and J.M.; data creation, A.T. and J.M.; writing—original draft preparation, Y.H.; project administration, Y.H.; funding acquisition, Y.H. All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

SF   Scale-Free
FVS   Feedback Vertex Set
NP   Non-deterministic Polynomial
BP   Belief Propagation
GC   Giant Component
RBR   Random Bypass Rewiring
GBR   Greedy Bypass Rewiring
SLR   Simple Local Repair

References

1. U.S.-Canada Power System Outage Task Force. Final Report on the 14 August 2003 Blackout in the United States and Canada: Causes and Recommendations. 2004. Available online: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf (accessed on 9 January 2021).
2. FINAL REPORT of the Investigation Committee on the 28 September 2003 Blackout in Italy. Available online: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/20040427_UCTE_IC_Final_report.pdf (accessed on 9 January 2021).
3. The Great East Japan earthquake: A story of a Devastating Natural Disaster, A Tale Of Human Compassion, 11 March 2011. World Health Organization, Western Pacific Region, December 2013. Available online: https://apps.who.int/iris/rest/bitstreams/920441/retrieve (accessed on 9 January 2021).
4. Amaral, L.; Scala, A.; Barthelemy, M.; Stanley, H.E. Classes of small-world networks. *Proc. Natl. Acad. Sci. USA* **2000**, *97*, 11149–11152. [CrossRef] [PubMed]
5. Barabási, A.-L.; Albert, R.; Jeong, H. Mean-filed theory for scale-free random networks. *Physica A* **2000**, *272*, 173–187. [CrossRef]
6. Albert, R.; Jeong, H.; Barabási, A.-L. Error and attack tolerance of complex networks. *Nature* **2000**, *406*, 378–382. [CrossRef] [PubMed]
7. Hollnagel, E.; Woods, D.-D.; Leveson, N. *Resilience Engineering-Concepts and Precepts*; ASHGATE Publishing: Farnham, UK, 2006.
8. Folke, C. Resilience: The Emergence of a Perspective for Social-Ecological Systems Analyses. *Glob. Environ. Chang.* **2006**, *16*, 253–267. [CrossRef]
9. Zolli, A.; Healy, A. *Resilience-Why Things Bounce Back*; Free Press: Wong Chuk Hang, Hong Kong, 2012.
10. Hayashi, Y.; Tanaka, A.; Matsukubo, J. Effective Self-Healing Networks against Attacks or Disasters in Resource Allocation Control. In Proceedings of the 12th International Conference on Adaptive and Self-Adaptive Systems and Applications (ADAPTIVE) (Online), Nice, France, 25–29 October 2020; pp. 85–91. ISBN 978-1-61208-781-8.
11. Schneider, C.M.; Moreira, A.A.; Andrade, J.S., Jr.; Havlin, S.; Herrmann, H.J. Mitigation of malicious attacks on networks. *Proc. Natl. Acad. Sci. USA* **2011**, *108*, 3838–3841. [CrossRef] [PubMed]
12. Tanizawa, T.; Havlin, S.; Stanley, H.E. Robustness of onion-like correlated networks against targeted attacks. *Phys. Rev. E* **2012**, *85*, 046109. [CrossRef] [PubMed]
13. Wu, Z.-X.; Holme, P. Onion structure and network robustness. *Phys. Rev. E* **2011**, *84*, 026106. [CrossRef] [PubMed]
14. Braunstein, A.; Dall'Asta, L.; Semerjiand, G.; Zdeborová, L. Network dismantling. *Proc. Natl. Acad. Sci. USA* **2016**, *113*, 12368–12373. [CrossRef] [PubMed]
15. Karp, R.M. Reducibility among combinatorial problems. In *Complexity of Computer Communications*; Miller, E., Thatcher, J.W., Bohlinger, J.D., Eds.; Plenum Press: New York, NY, USA, 1972; pp. 85–103. [CrossRef]
16. Hayashi, Y. Growing Self-organized Design of Efficient and Robust Complex Networks. In Proceedings of the 8th IEEE International Conference on Self-Adaptive and Self-Organizing Systems (SASO), London, UK, 8–12 September 2014.
17. Hayashi, Y. A new design principle of robust onion-like networks self-organized in growth. *Netw. Sci.* **2018**, *6*, 54–70. [CrossRef]
18. Hayashi, Y.; Uchiyama, N. Onion-like networks are both robust and resilient. *Sci. Rep.* **2018**, *8*, 11241. [CrossRef] [PubMed]
19. Chujyo, M.; Hayashi, Y. A loop enhancement strategy for network robustness. *Appl. Netw. Sci.* **2021**, *6*, 1–13. [CrossRef]
20. Song, S.; Park, H.; Choi, B.-Y.; Zhu, H. Control path management framework for enhancing software-defined network (SDN) reliability. *IEEE Trans. Netw. Serv. Manag.* **2017**, *4*, 302–316. [CrossRef]
21. Hu, Y.; Wendong, W.; Gong, X.; Que, X.; Shiduan, C. Reliability-aware controller placement for software-defined networks. In Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, Ghent, Belgium, 27–31 May 2013; pp. 672–675. [CrossRef]
22. Thyagaturu, A.S.; Mercian, A.; McGray, P.; Reisslein, M.; Kellerer, W. Software defined optical networks (SDONs): A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2738–2786. [CrossRef]
23. Zhou, H.-J. Spin glass approach to the feedback vertex set problem. *Eur. Phys. J. B* **2013**, *86*, 455. [CrossRef]
24. Park, J.; Hahn, S.G. Bypass rewiring and robustness of complex networks. *Phy. Rev. E* **2016**, *94*, 022310. [CrossRef] [PubMed]
25. Gallos, L.K.; Fefferman, N.H. Simple and efficient self-healing strategy for damaged complex networks. *Phy. Rev. E* **2015**, *92*, 052806. [CrossRef] [PubMed]

26. Stippinger, M.; Kertész, J. Enhancing resilience of interdependent networks by healing. *Physica A* **2014**, *416*, 481–487. [CrossRef]
27. Hayes, T.; Rustagi, N.; Saia, J.; Trehan, A. The Forgiving Tree: A Self-Healing Distributed Data Structure. In Proceedings of the 27th ACM Symposium on Principles of Distributed Computing (PODC), Toronto, ON, Canada, 18–21 August 2008; pp. 203–212. ISBN 978-1-59593-989-0. Available online: https://dl.acm.org/citation.cfm?doid=1400751.1400779 (accessed on 9 January 2021). [CrossRef]
28. Castañeda, A.; Dolev, D.; Trehan, A. Compact routing messages in self-healing. *Theor. Comput. Sci.* **2018**, *709*, 2–19. [CrossRef]
29. Data Source of Real Infrastructure Networks. OpenFlights. Available online: http://networkrepository.com/inf-openflights.php (accessed on 9 January 2021).
30. Internet AS Oregon. Available online: http://snap.stanford.edu/data/as.html (accessed on 9 January 2021).
31. US PowerGrid. Available online: http://www-personal.umich.edu/~mejn/netdata/power.zip (accessed on 9 January 2021).