# Effective Self-Healing Networks against Attacks or Disasters in Resource Allocation Control

Yukio Hayashi

Graduate School of Advanced
Institute of Science and Technology,
Japan Advanced Institute of
Science and Technology
Nomi-city, Ishikawa 923-1292
Email: yhayashi@jaist.ac.jp

Atsushi Tanaka

Department of Informatics and Electronics
Faculty of Engineering,
Yamagata University
Yonezawa-city, Yamagata 992-8510
Email: tanaka@yamagata-u.ac.jp

Jun Matsukubo

Department of Creative Engineering,
National Institute of Technology
Kitakyushu College
Kitakyushu-city, Fukuoka 802-0985
Email: jmatsu@apps.kct.ac.jp

***Abstract*—With increasing threats by large attacks or disasters, the time has come to reconstruct network infrastructures such as communication or transportation systems rather than to recover them as before in case of accidents, because many real networks are extremely vulnerable. Thus, we consider self-healing mechanisms by rewirings (reuse or addition of links) to be sustainable and resilient networks even against malicious attacks. In distributed local process for healing, the key strategies are the extension of candidates of linked nodes and enhancing loops by applying a message-passing algorithm inspired from statistical physics. Simulation results show that our proposed combination of ring formation and enhancing loops is particularly effective in comparison with the conventional methods, when more than half damaged links work or are compensated from reserved ones.**

***Keywords*–Self-Healing; Complex Network Science; Connectivity; Enhancing Loops; Message-Passing Algorithm; Resource Allocation; Resilience.**

## I. INTRODUCTION

In contemporary world, network infrastructures, such as communication, trading, transportation, energy and water supply systems are crucial for supporting social activities, economy, industrial production, etc., while increasing the frequency of large disasters or military conflicts turn threats by destroying the functions into reality. To confront the serious problems, a new supple approach *resilience* [1][2] attracts much attention in system engineering, biology, ecology, and sociology. Resilience means the ability to sustain basic objective and integrity even in encountering with the extreme change of situations or environments (e.g., by disasters or malicious attacks) for technological system, organization, or individual [1]. However, to be resilient system, the concept of safety against accidents or disruptions should be extended from *Safety-I* to *Safety-II* [3]: from “as few things as possible go wrong” to “as many things as possible go right”, from “reactive, respond when something happens” to “proactive, continuously trying to anticipate developments and events”, and so on, in these two complementary views, which do not conflict. Safety-II requires to adjust, adapt, develop, and design better processes with technological or human resource allocations. Moreover, the concept of resilience includes reorganization or reconstruction of the system with adaptive capacity beyond the conventional recovery [4], as shown in Table I. Such paradigm shift has affinity to self-adaptive mechanism or system. Thus, we focus on developing new mechanism to lead to (social-ecological) resilience with reconstruction as far as accepting innovation rather than finding and decreasing weak or wrong parts in a network system.

TABLE I. A SEQUENCE OF RESILIENCE CONCEPTS WHICH ARE PARTIALLY EXTRACTED FROM [4].

| *Resilience concept* | *Characteristics* | *Focus on* |
|---|---|---|
| Engineering resilience | Return time, efficiency | Recovery, constancy |
| Ecological/ecosystem resilience | Buffer capacity, withstand shock, maintain function | Persistence, robustness |
| Social−ecological resilience | Interplay disturbance and **reorganization**, sustaining and developing | **Adaptive capacity**, transformability, learning, innovation |

In this paper, we study how to reconstruct a sustainable network under limited resource, and propose effective self-healing methods based on enhancing loops through a local process around damaged parts. The motivations for enhancing loops are as follows. There is a common topological structure called Scale-Free (SF) in many social, biological, and technological networks [5][6]. Although the SF networks have an extreme vulnerability against malicious attacks [7], it has been found that onion-like structure with positive degree-degree correlations gives the optimal robustness of connectivity [8][9]. Onion-like structure can be generated by whole rewiring [8][10] in enhancing the correlations under a given degree distribution. Moreover, since dismantling and decycling problems are asymptotically equivalent at infinite graphs in a large class of random networks with light-tailed degree distribution [11], a tree remains without loops at the critical state before the complete fragmentation by node removals. Dismantling (or decycling) problem known as NP-hard [12] is to find the minimum set of nodes in which removal leaves a graph broken into connected components whose maximum size is at most a constant (or a graph without loops). It is suggested that the robustness becomes stronger as many loops exist as possible. In fact, to be onion-like networks, enhancing loops by copying or intermediation is effective for improving the robustness in incrementally growing methods [13][14] based on a local distributed process. Thus, we remark that loops make bypasses and may be more important than the degree-degree correlations in order to improve the connectivity in a network reconstruction after large disasters or attacks. However, identifying the necessary nodes to form loops is intractable due to combinatorial NP-hardness, we effectively apply an approximate calculation based on a statistical physics approach in our proposed self-healing. We assume that rewirings (reuse of undestroyed links) are performed by changing directions or ranges of flight routes or wireless beams in the healing process, though we do not discuss the detail realization that depends on the current or future technologies and target systems.

The organization of this paper is as follows. In Section 2, we introduce the conventional methods for recovery and healing of a damaged network, and newly discuss some limitations and extensions of the resource for connecting nodes. In Section 3, we explain our proposed self-healing method. In Section 4, we show the effect of healing on the connectivity and the efficiency of paths in damaged real networks by malicious attacks through computer simulation. In Section 5, we summarize the obtained results and mention a future work.

## II. Related Work

We briefly review recent progress of typical methods for recovery and healing of a network in complex network science (inspired from fractal statistical physics) and computer science.

In complex network science, several recovery and healing methods have been proposed. As one of the recovery methods, the strategies of random, greedy (for regaining the largest connectivity), and preferential recovery weighted by population have been considered in taking into account the order of recovered links [15]. The effectiveness of recovery from localized attacks is investigated on a square lattice. Against link failures, a simple recovery method has been also introduced to reconstruct an active tree for delivering from a source node by using back-up links [16]. However, it is unclear which pairs of two nodes should be prepared for back-up links in advance.

On the other hand, a self-healing method has been proposed by establishing new random links on interdependent (two-layered) networks of square lattices [17], and the effect against node attacks is numerically studied. In particular, for adding links by the healing process, the candidates of linked nodes are incrementally extended from only the direct neighbors of the removed node by attacks until no more separation of components occurs. In other words, the whole connectivity is maintained except the isolating removed parts (known as induced sub-graphs for removed nodes in computer science). Note that such an extension of the candidates of linked nodes is a key idea in our proposed self-healing method as mentioned later.

Furthermore, the following self-healing methods, whose effects are investigated for some data of real networks, are worthy to note. One is a distributed local repair in order of a priority to the most damaged node [18]. In the repair by linking from the most damaged node to a randomly chosen node from the unremoved node set in its next-nearest neighbors before attacks, the order of 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 $k_{dam}/k_{orig}$ exceeds a threshold. Another is a bypass rewiring [19] on more limited resource of links (wire cables, wireless communication or transportation lines between two nodes) and ports (channels or plug sockets at a node). To establish links between pair nodes, a node is randomly chosen only one time in the neighbors of each removed node. When $k_i$ denotes the degree of removed node $i$, only $\lfloor k_i/2 \rfloor$ links are reused. Note that a degree represents the number of using ports at the node. In the bypass rewiring, reserved additional ports are not necessary: they do not exceed the original one before attacks. Moreover, greedy bypass rewiring [19] is proposed in order 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, ForgivingTree algorithm has been proposed [20]. Under the 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). It is based on both distributed process of sending messages and data structure, furthermore developed to an efficient algorithm called as compact routing [21]. In each rewiring process, a removed node and its links are replaced by a binary tree. 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 is unnecessary. It is remarkable for computation (e.g., in routing or information spreading) that the multiplicative factor of 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 replacing 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 disconnected into subtrees by any attack to the joint node. In other research, a recovery strategy with resource allocation of bandwidth in a communication network is discussed at several service levels from full to partial with respect to what and how optimization [22], although considering the link's thickness (e.g., defined by bandwidth or transportation amounts) is out of our current scope.

TABLE II. Reserved resource at a node in self-healing methods.

| *Method* | *Additional links* | *Additional ports* |
|---|---|---|
| ForgivingTree [20] | Unnecessary,<br>enough by the original<br>under the reuse | Two or three at most<br>in a binary tree |
| Bypass Rewiring [19] | Unnecessary,<br>if about half is reusable<br>from the original | Unnecessary,<br>enough by the original |
| Simple Local Repair [18] | Controllable by<br>$f_s(1-q)N$ | Necessary<br>according to $f_s$<br>and attack rate $q$ |
| Our Proposed Method | Controllable by<br>$M_h$ | Necessary<br>according to $r_h$<br>and attack rate $q$ |

The characteristics of resource allocation are summarized in Table II for the above conventional and our proposed methods, although there has been no discussion about resource of links and ports. ForgivingTree or bypass rewiring methods is not controllable but strongly depending on the reuse of all or half links before attacks. We assume that some links emanated from a removed node $i$ can be reused for healing by local rewiring between the neighbors. These links (cable lines) work at the neighbor's sides, even though they are disconnected at the removed node's side. As a control parameter in our simulation, we set the reusable rate $r_h$ according to the damage, on the assumption $k_i(1-r_h)$ links do not work in the removed node's degree $k_i$. In the two kinds of resource, we consider that ports work independently from connection links, as similar to a relation of airport runaway (or plug socket) and flight by airplane (or cable line). As one of the added values from the conventional heuristic methods, we consider a new design strategy by enhancing loops to improve the effect on healing in the next section.

## III. Effective Self-Healing

### A. Outline of Proposed Methods

We assume that almost simultaneously attacked nodes are not recoverable immediately, therefore are removed from the network function for a while. In case of emergency for healing, unconnected two nodes are chosen and rewired as the reconstruction assistance or reuse of links emanated from removed $qN$ nodes, when the fraction of attacks is $q$. The healing process in each of the following 1), 2), and 3) is initiated just after detecting attacks and repeated by $M_h \overset{\text{def}}{=} r_h \times \tilde{\sum}_{i\in D_q} k_i$ links. Here, $\tilde{\sum}_{i\in D_q} k_i$ means the number without multiple counts of lost links by attacks. $D_q$ denotes the set of removed nodes, $|D_q| = qN$. The key strategies are 1) enhancing loops contributes to improve the robustness [14][23], 2) forming a ring that encloses damaged parts is able to maintain the connectivity on the edges of extended neighbors, and 3) complementary effects of 1) and 2) in the limited resource of $M_h$ links. Any one of them is performed as the healing process.

1) Enhancing loops for smaller $q_j^0 + q_{j'}^0$
To select two nodes in the neighbor nodes $j, j' \in \partial i$ in the increasing order of $q_j^0 + q_{j'}^0$ for all $i \in D_q$, as shown in Figure 1.

2) Extended ring
To make a ring of simple cycle without crossing, the neighbors are extended from the first damaged, the second damaged, etc., to the last damaged area in this order, as shown in Figure 2.

3) Combination of extended ring & enhancing loops for smaller $q_j^0 + q_{j'}^0$
After using $M_r \leq \tilde{\sum}_{i\in D_q} k_i$ links for the ring, if $M_h > M_r$, then the selections of two nodes in the extended neighbors on ring are repeated in the increasing order of $q_j^0 + q_{j'}^0$ for $M_h - M_r$ links. Else a ring is incomplete and an open chain is generated among the extended neighbors. In this case, additional rewirings between the nodes $j, j'$ with smaller $q_j^0 + q_{j'}^0$ are not performed due to lack of links.

Enhancing loops is performed by applying the values of $q_i^0$ (introduced in next subsection) for estimating Feedback Vertex Set (FVS) whose nodes are necessary to form loops. Since a node $i$ with small $q_i^0$ belongs to a dangling subtree with high probability, by connecting such nodes, it is expected that a new loop on which a part of the subtree is included is added. From left to right in Figure 1, the original red links emanated from the removed node $i$ (marked by filled circle) are reused as the blue ones for the healing. When there is at least a path between the nodes $j$ and $j'$ in Figure 1, a new loop is created. Note that the attacked node $i$ is isolatedly removed as breakdown.

A ring is generated as follows. In Figure 2, the process is initiated in order of removals of three nodes from left to right. Filled and open circles denote removed and active nodes, red and magenta lines denote removed and virtually added links, respectively. From top left to top right in Figure 2, a red node and its links are damaged, a ring formation around the 1st removal node at the left is tried to the direct neighbors of it. A green link is established, while virtual magenta links are considered by sending messages to active neighbors. From middle left to middle right in Figure 2, the ring formation around the 2nd removal node at the center is tried again to the neighbors which include the extended ones by the virtual links. Light blue links are added, but virtual magenta links are considered. From bottom left to bottom right in Figure 2, the ring formation around the 3rd removal node at the right is tried similarly. Finally, a ring is established by green, light blue, and blue links. The connections between neighbors on a ring are in random order except through the extension process.

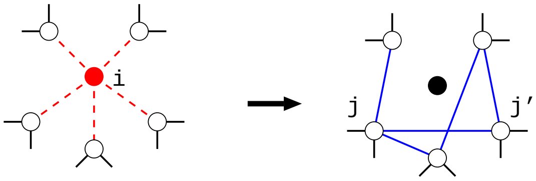

Figure 1. Rewiring between nodes with small $q_j^0 + q_{j'}^0$.

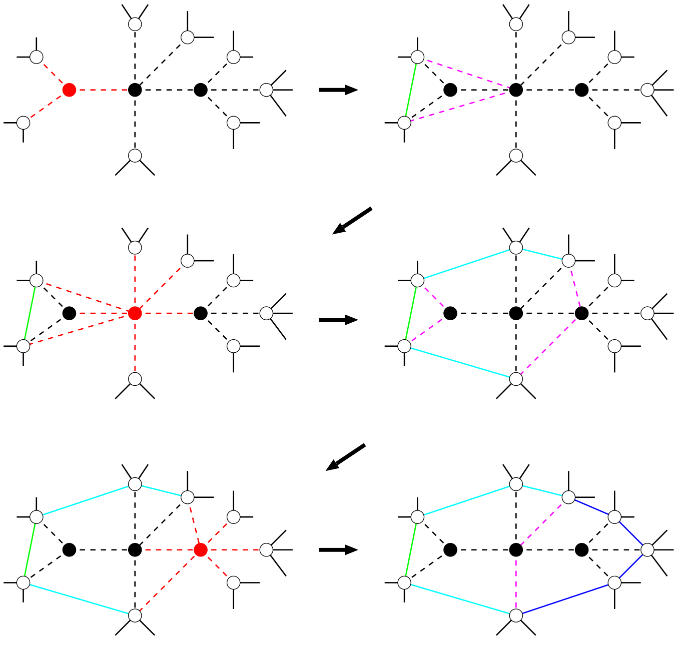

Figure 2. Generation process of a ring.

### B. Applying Belief Propagation Algorithm

We review the following approximation algorithm [24][25] derived for estimating FVS known as NP-hard problem [12]. It is based on a cavity method in statistical physics in the assumption that nodes $j \in \partial i$ are mutually independent of each other when node $i$ is removed. The joint probability is $\mathcal{P}_{\setminus i}(A_j : j \in \partial i) \approx \Pi_{j \in \partial i} q_{j \to i}^{A_j}$ by the product of independent marginal probability $q_{j \to i}^{A_j}$ for the state $A_j$ as the index of $j$'s root. In the cavity graph, if all nodes $j \in \partial i$ are either empty ($A_j = 0$) or roots ($A_j = j$), the added node $i$ can be a root ($A_i = i$). There are the following exclusive states.

1) $A_i = 0$: $i$ is empty (removed). Since $i$ is unnecessary as a root, it belongs to FVS.
2) $A_i = i$: $i$ becomes its own root. The state $A_j = j$ of $j \in \partial i$ is changeable to $A_j = i$ when node $i$ is added.
3) $A_i = k$: one node $k \in \partial i$ becomes the root of $i$ when it is added, if $k$ is occupied and all other $j \in \partial i$ are either empty or roots.

The corresponding probabilities to the above three states are represented by

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

$$q_i^i \overset{\text{def}}{=} \frac{e^x \Pi_{j \in \partial i(t)} \left[ q_{j \to i}^0 + q_{j \to i}^j \right]}{z_i(t)},$$

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

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

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

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

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

$$\begin{aligned} z_{i \to j}(t) \quad &\overset{\text{def}}{=} \quad 1 + e^x \Pi_{k \in \partial i(t) \setminus j} \left[ q_{k \to i}^0 + q_{k \to i}^k \right] && (5) \\ &\times \left[ 1 + \sum_{l \in \partial i(t) \setminus j} \frac{1 - q_{l \to i}^0}{q_{l \to i}^0 + q_{l \to i}^l} \right], && (6) \end{aligned}$$

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

$$q_i^0 + q_i^i + \sum_{k \in \partial i} q_i^k = 1,$$

$$q_{i \to j}^0 + q_{i \to j}^i + \sum_{k \in \partial i} q_{i \to j}^k = 1.$$

The message-passing iterated by equations (1)-(6) is called Belief Propagation (BP). These calculations of $q_i^0$, $q_i^i$, $q_i^k$, $q_{i \to j}^0$, $q_{i \to j}^i$, and $q_{i \to j}^k$ are locally executed through the message-passing until to be self-consistent in principle but practically to reach appropriate rounds from initial setting of $(0, 1)$ random values. The unit time from $t$ to $t + 1$ for calculating a set $\{q_i^0\}$ consists of a number of rounds by updating equations (1)-(6) in order of random permutation of the total $N$ nodes. The distributed calculations can be also considered.

## IV. Simulation Results

We evaluate the effect of healing by two measures: the ratio $\frac{S(q)}{(1-q)N}$ [18] for the connectivity and the efficiency $E \overset{\text{def}}{=} \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{L_{ij}}$, where $S(q)$ and $L_{ij}$ denote the size of GC (giant component or largest connected cluster) and the length of the shortest path counted by hops between $i$-$j$ nodes, respectively, for a network after removing $qN$ nodes by attacks with recalculation of the highest degree node as the target. We investigate them for Open Flight between airports and Internet AS Oregon as examples of real networks [26], whose number of nodes and links are $N = 2905$, $M = 15645$, and $N = 6474$, $M = 12572$. The following results are averaged over 10 samples with random process for tie-breaking in a node selection or ordering of nodes on a ring.

TABLE III. NUMBER OF ADDITIONAL PORTS IN OUR PROPOSED COMBINATION METHOD FOR THE FRACTION $q$ OF ATTACKS AND THE REUSABLE RATE $r_h$ OF LINKS.

Open Flight: $k_{max} = 242$

| $q$<br>$r_h$ | *0.1* | *0.2* | *0.3* | *0.4* | *0.5* | *0.6* | *0.7* | *0.8* | *0.9* |
|---|---|---|---|---|---|---|---|---|---|
| 0.05 | 1.0<br>( 0.3) | 1.0<br>( 0.4) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 32.8<br>( 1.4) | 73.2<br>( 4.6) |
| 0.1 | 1.0<br>( 0.4) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 18.2<br>( 0.7) | 80.8<br>( 1.4) | 194.1<br>( 2.3) | 246.7<br>( 4.1) | 203.5<br>( 9.0) |
| 0.2 | 89.2<br>( 1.0) | 84.7<br>( 1.5) | 294.3<br>( 1.7) | 347.0<br>( 2.3) | 362.0<br>( 3.1) | 446.5<br>( 4.0) | 412.5<br>( 5.8) | 341.1<br>( 9.0) | 228.2<br>(19.1) |
| 0.5 | 253.1<br>( 4.8) | 244.0<br>( 6.3) | 636.4<br>( 6.3) | 671.6<br>( 7.5) | 726.6<br>( 9.2) | 584.1<br>(11.8) | 539.8<br>(15.9) | 407.9<br>(24.3) | 233.0<br>(50.8) |
| 1.0 | 403.0<br>(10.9) | 449.4<br>(13.8) | 807.8<br>(14.1) | 822.1<br>(16.1) | 755.8<br>(19.5) | 626.7<br>(24.6) | 571.2<br>(33.3) | 422.4<br>(50.9) | 249.2<br>(103.4) |

As Oregon: $k_{max} = 1458$

| $q$<br>$r_h$ | *0.1* | *0.2* | *0.3* | *0.4* | *0.5* | *0.6* | *0.7* | *0.8* | *0.9* |
|---|---|---|---|---|---|---|---|---|---|
| 0.05 | 1.0<br>( 0.4) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.6) | 1.0<br>( 0.6) | 1.0<br>( 0.5) | 1.0<br>( 0.5) |
| 0.1 | 1.0<br>( 0.5) | 1.0<br>( 0.6) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 147.4<br>( 2.5) |
| 0.2 | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 1.0<br>( 0.5) | 176.9<br>( 1.1) | 440.1<br>( 2.4) | 473.7<br>( 6.1) |
| 0.5 | 70.1<br>( 0.7) | 289.1<br>( 1.0) | 509.4<br>( 1.3) | 824.6<br>( 1.8) | 1112.4<br>( 2.4) | 1252.7<br>( 3.3) | 1122.7<br>( 4.9) | 820.1<br>( 8.1) | 485.1<br>(17.7) |
| 1.0 | 248.9<br>( 3.0) | 2275.3<br>( 3.3) | 2002.8<br>( 4.0) | 1801.2<br>( 4.9) | 1575.7<br>( 6.2) | 1343.0<br>( 8.2) | 1068.0<br>(11.4) | 822.8<br>(17.8) | 494.6<br>(37.1) |

TABLE IV. NUMBER OF ADDITIONAL PORTS IN THE CONVENTIONAL SIMPLE LOCAL REPAIR METHOD FOR THE FRACTION $q$ OF ATTACKS AND THE REUSABLE RATE $r_h$ OF LINKS.

Open Flight: $k_{max} = 242$

| $q$<br>$r_h$ | *0.1* | *0.2* | *0.3* | *0.4* | *0.5* | *0.6* | *0.7* | *0.8* | *0.9* |
|---|---|---|---|---|---|---|---|---|---|
| 0.05 | 14.9<br>(2.5) | 8.1<br>(1.5) | 8<br>(1.3) | 8.7<br>(1.5) | 8.3<br>(1.4) | 9.1<br>(1.5) | 10.6<br>(1.5) | 9.2<br>(1.5) | 7.1<br>(1.4) |
| 0.1 | 14.6<br>(2.0) | 8.2<br>(1.5) | 11.6<br>(1.5) | 9.2<br>(1.5) | 8.5<br>(1.5) | 10.1<br>(1.5) | 8.9<br>(1.5) | 7.7<br>(1.5) | 6<br>(1.4) |
| 0.2 | 7.6<br>(1.4) | 9.3<br>(1.5) | 10.3<br>(1.5) | 11.8<br>(1.5) | 11.1<br>(1.5) | 10.8<br>(1.5) | 8.8<br>(1.5) | 8.6<br>(1.5) | 6.7<br>(1.4) |
| 0.5 | 7.6<br>(1.4) | 9.3<br>(1.5) | 10.3<br>(1.5) | 11.8<br>(1.5) | 11.1<br>(1.5) | 10.8<br>(1.5) | 8.8<br>(1.5) | 8.6<br>(1.5) | 6.7<br>(1.4) |
| 1.0 | 7.6<br>(1.4) | 9.3<br>(1.5) | 10.3<br>(1.5) | 11.8<br>(1.5) | 11.1<br>(1.5) | 10.8<br>(1.5) | 8.8<br>(1.5) | 8.6<br>(1.5) | 6.7<br>(1.4) |

AS Oregon: $k_{max} = 1458$

| $q$<br>$r_h$ | *0.1* | *0.2* | *0.3* | *0.4* | *0.5* | *0.6* | *0.7* | *0.8* | *0.9* |
|---|---|---|---|---|---|---|---|---|---|
| 0.05 | 4.5<br>(1.1) | 4.4<br>(1.2) | 4.3<br>(1.2) | 5.3<br>(1.2) | 5<br>(1.3) | 5.2<br>(1.3) | 6.4<br>(1.4) | 7.6<br>(1.5) | 6.6<br>(1.5) |
| 0.1 | 5.8<br>(1.3) | 5.9<br>(1.3) | 5.8<br>(1.4) | 6<br>(1.4) | 7.1<br>(1.4) | 7.1<br>(1.5) | 7.6<br>(1.5) | 7.9<br>(1.5) | 6.9<br>(1.5) |
| 0.2 | 7.9<br>(1.4) | 7.8<br>(1.5) | 7.9<br>(1.5) | 8.7<br>(1.5) | 9.5<br>(1.5) | 9<br>(1.5) | 7.4<br>(1.5) | 7.3<br>(1.5) | 7.3<br>(1.5) |
| 0.5 | 8.6<br>(1.5) | 9<br>(1.5) | 9.5<br>(1.5) | 9.2<br>(1.5) | 9.1<br>(1.5) | 9<br>(1.5) | 7.4<br>(1.5) | 8.2<br>(1.5) | 6.9<br>(1.5) |
| 1.0 | 8.6<br>(1.5) | 9<br>(1.5) | 9.5<br>(1.5) | 9.2<br>(1.5) | 9.1<br>(1.5) | 9<br>(1.5) | 7.4<br>(1.5) | 8.2<br>(1.5) | 6.9<br>(1.5) |

Figure 3 shows the ratio of GC in the surviving nodes which may be divided into isolated clusters after attacks. The number $M_h$ of rewiring is controlled by a parameter $r_h$ in the healing. Red, green, blue, orange, and purple lines correspond to the reusable rate of links $r_h = 0.05$, 0.1, 0.2, 0.5, and 1.0. Black line shows the result for no healing. In comparison with

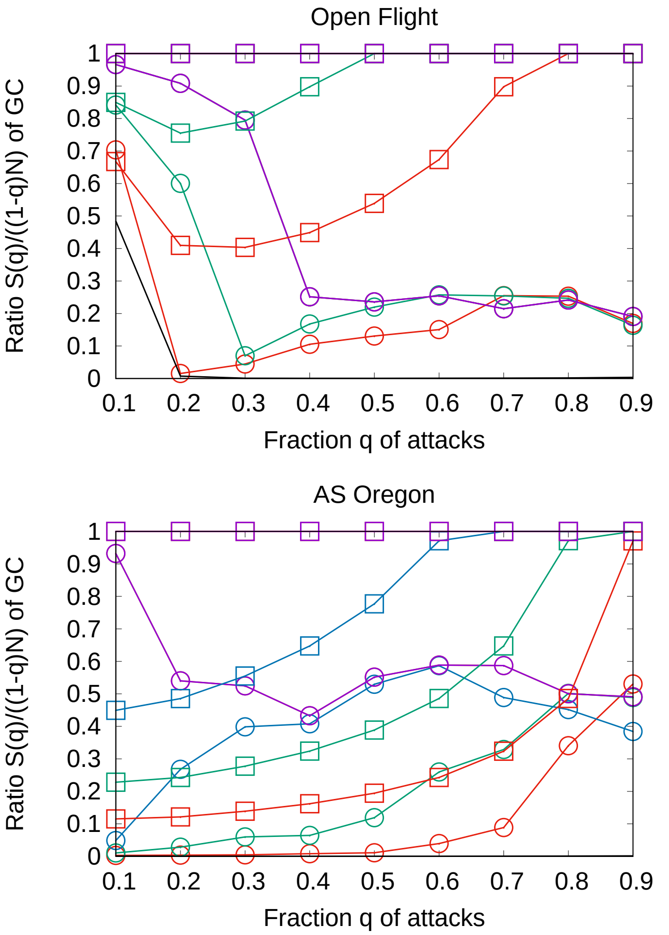

Figure 3. Communicable or transportable size with healing by our proposed combination (square) and conventional simple local repair (circle). Red, green, blue, orange, and purple lines correspond to the reusable rate $r_h = 0.05$, 0.1, 0.2, 0.5, and 1.0. Black line shows the result for no healing.

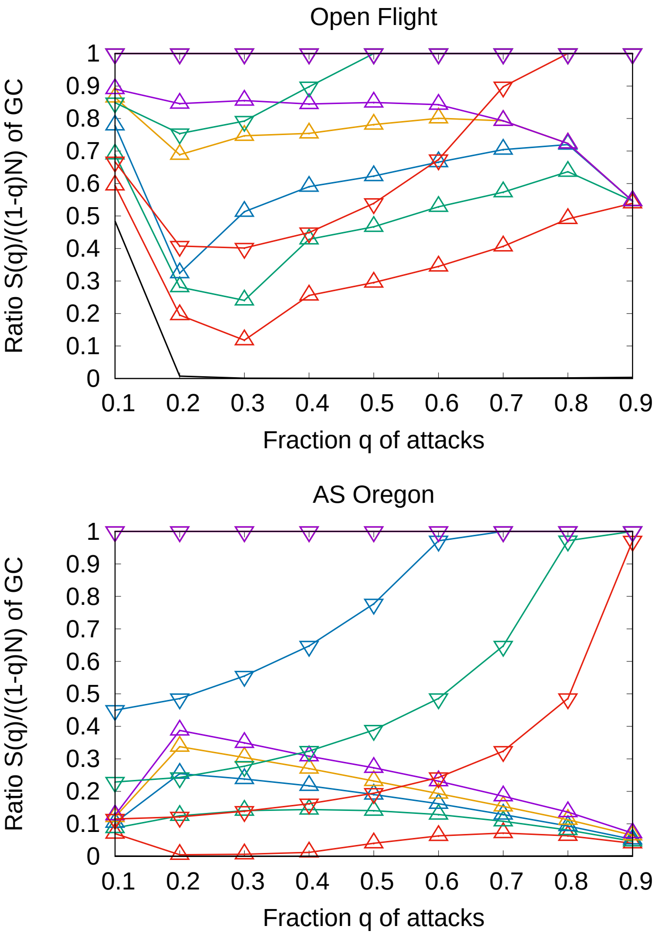

Figure 4. Communicable or transportable size with healing by only enhancing loops (up triangle) or extended ring (down triangle). Red, green, blue, orange, and purple lines correspond to the reusable rate $r_h = 0.05$, 0.1, 0.2, 0.5, and 1.0. Black line shows the result for no healing.

same color lines, our proposed combination method (marked by square) of extended ring and enhancing loops is superior with higher ratio than the conventional simple local repair [18] method (marked by circle) with a priority of rewirings to more damaged nodes, whose healing works only for weak attacks in small $q$. We remark that in our proposed combination method the cases of $r_h \geq 0.5$ (overlapped orange and purple lines marked by square) maintains the almost whole connectivity in the surviving $(1-q)N$ nodes. In other words, the network function can be revived completely, if more than half of links emanated from removed nodes work. In $r_h \leq 0.1$ (green and red lines marked by square), making a ring is unfinished, the ratio is dropped. Moreover, since the ratio in Figure 4 is lower than the ratio marked by square in Figure 3, only enhancing loops (marked by up-pointing triangle) or extended ring (marked by down-pointing triangle) has weaker effect than the combination. However, enhancing loops increase the ratio of GC moderately in $r_h \leq 0.1$ for $q \leq 0.5$ (green and red lines marked by up-pointing triangle) in Figure 4.

As shown in Figures 5 and 6, our proposed combination method (marked by square) has higher efficiency of paths than the conventional simple local repair method (marked by circle) in comparison with same color lines, although the effect in the method by only enhancing loops (marked by up-pointing triangle) or extended ring (marked by down-pointing triangle) becomes weaker with $E < 0.3$. Dotted line shows the efficiency in the original network before attacks.

On the other hand, we investigate the number of additional ports which should be prepared in advance besides reusable ports. It is reasonable to consider that the original ports at neighbors of a removed node remain and can be reused at undamaged locations, even if the links from the neighbors are disconnected on the way. Thus, we assume that there exist active ports of a node at least as many as its degree in the original network before attacks. Note that the minimum, average, and maximum degrees are $k_{min} = 1$, $\langle k \rangle = 10.77$, and $k_{max} = 242$ in Open Flight, $k_{min} = 1$, $\langle k \rangle = 3.88$, and $k_{max} = 1458$ in AS Oregon. Table III shows the maximum number of reserved additional ports in our proposed combination method. The number tends to be larger ranging from a few to nearly $2k_{max} \sim 3k_{max}$, as the fraction $q$ of attacks and the reusable rate $r_h$ increase. Shown in parentheses are averaged values over the nodes that require additional ports in each network with healing. The averaged number of

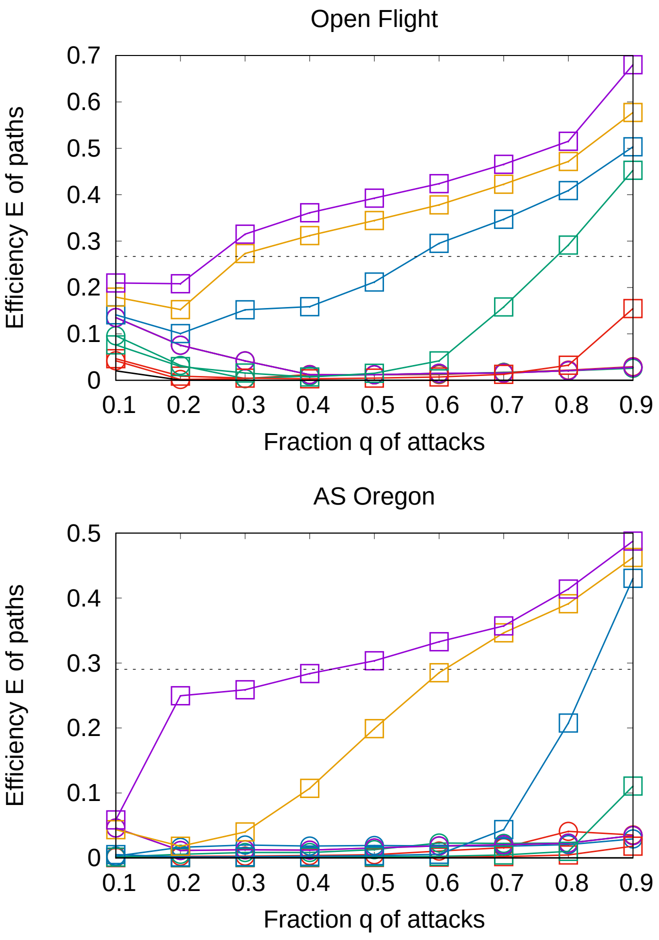

Figure 5. Efficiency of paths in the network with healing by our proposed combination (square) and conventional simple local repair (circle). Red, green, blue, orange, and purple lines correspond to the reusable rate $r_h = 0.05$, 0.1, 0.2, 0.5, and 1.0. Black line shows the result for no healing. Dotted line is the original level before attacks.

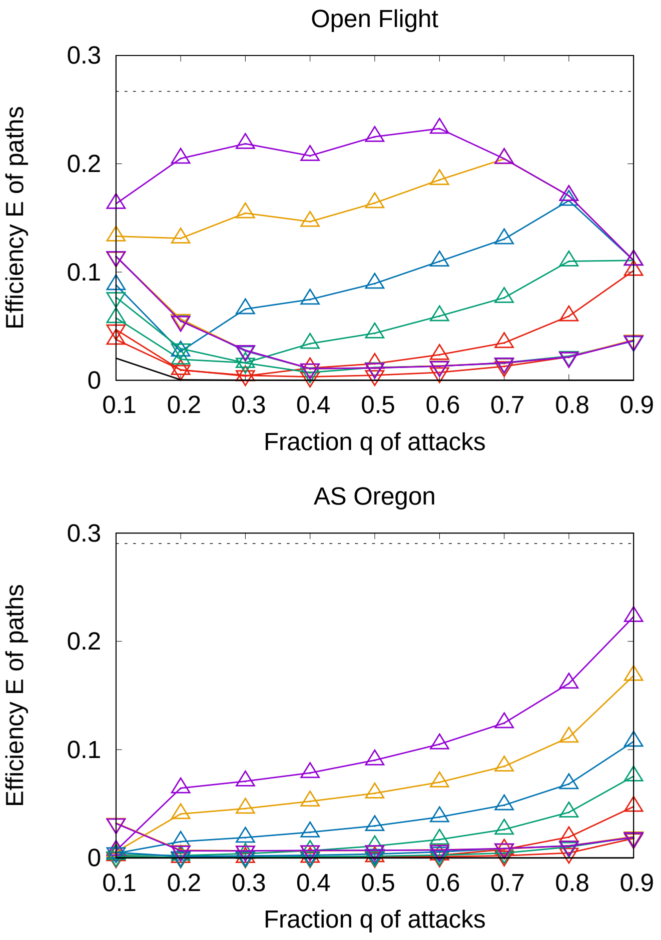

Figure 6. Efficiency of paths in the network with healing by only enhancing loops (up triangle) or extended ring (down triangle). Red, green, blue, orange, and purple lines correspond to the reusable rate $r_h = 0.05$, 0.1, 0.2, 0.5, and 1.0. Black line shows the result for no healing. Dotted line is the original level before attacks.

additional ports is small, thus the cost of resource is so much inexpensive. While the number is small even for the maximum in the conventional simple local repair method as shown in Table IV. It is almost constant for varying $r_h$ and $q$.

## V. Conclusion and Future Work

We have proposed self-healing methods for reconstructing a sustainable network by rewirings against attacks or disasters in the meaning of resilience with adaptive capacity. The fundamental rewiring mechanisms are based on maintaining the connectivity on a ring and enhancing loops for improving the robustness by applying BP algorithm inspired from statistical physics. As the resource allocation, the rewirings are controlled by a parameter $r_h$ for reuse or addition of links between the extended neighbors of attacked nodes. We have shown that our proposed method is better than the conventional simple local repair method [18] with a priority of rewirings to more damaged nodes, although reserved additional ports are required much more. In particular, the whole connectivity can be revived with high efficiency of paths in our proposed method, when more than half links emanated from attacked nodes work. Thus, such amount of links are necessary for sustaining network function. If there is lack of the resource, the shortage parts should be compensated according to the damages. Under the same resource, further improvement for both connectivity and efficiency with fewer additional ports by a modification of the proposed healing method will be a future work.

## Acknowledgment

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

## References

[1] A. Zolli and A. Healy, Eds., Resilience -Why Things Bounce Back-. Free Press, Jul. 2012, ISBN: 10: 1451683804.

[2] E. Hollnagel, D. Woods, and N. Leveson, Eds., Resilience Engineering -Concepts and Precepts-. CRC Press, Jan. 2006, ISBN: 10: 0754646416.

[3] E. Hollnagel, Ed., Safety-I and Safety-II -The Past and Future of Safety Management-. CRC Press, Apr. 2014, ISBN: 10: 13: 978-1472423054.

[4] C. Folke, "Resilience: The emergence of a perspective for social-ecological systems analyses," Global Environmental Change, vol. 16, 2006, pp. 253–267, DOI: 10.1016/j.gloenvcha.2006.04.002.

[5] L. Amaral, A. Scala, M. Barthelemy, and H. E. Stanley, “Classes of small-world networks,” Proc. Natl. Acad. Sci. USA, vol. 97, no. 21, 2000, pp. 11 149–11 152, DOI: 10.1073/pnas.200327197.

[6] A.-L. Barabási, “Scale-Free Networks,” Scientific American, vol. 288, no. 5, 2003, pp. 60–69, DOI: 10.1038/scientificamerican0503-60.

[7] R. Albert, H. Jeong, and A.-L. Barabási, “Error and attack tolerance of complex networks,” Nature, vol. 406, 2000, pp. 378–382, DOI: 10.1038/35019019.

[8] C. M. Schneider, A. A. Moreira, J. Andrade, Jr., and H. J. Herrmann, “Mitigation of malicious attacks on networks,” Proc. Natl. Acad. Sci. USA, vol. 108, no. 10, 2011, pp. 3838–3841, DOI: 10.1073/pnas.1009440108.

[9] T. Tanizawa, S. Havlin, and H. E. Stanley, “Robustness of onion-like correlated networks against targeted attacks,” Physical Review E, vol. 85, no. 046109, 2012, pp. 1–9, DOI: 10.1103/PhysRevE.85.046109.

[10] Z.-X. Wu and P. Holme, “Onion structure and network robustness,” Physical Review E, vol. 84, no. 026106, 2011, pp. 1–5, DOI: 10.1103/PhysRevE.84.026106.

[11] A. Braunstein, L. Dall’Asta, G. Semerjiand, and L. Zdeborová, “Network dismantling,” Proc. Natl. Acad. Sci. USA, vol. 113, no. 44, 2016, pp. 12 368–12 373, DOI: 10.1073/pnas.1605083113.

[12] R. M. Karp, Reducibility among combinatorial problems. Springer, Boston, MA, 1972, pp. 85–103, the IBM Research Symposia Series, ISBN: 978-1-4684-2003-6.

[13] Y. Hayashi, “Growing Self-organized Design of Efficient and Robust Complex Networks,” IEEE Xplore Digital Library SASO (Self-Adaptive and Self-Organizing systems) 2014, 2014, pp. 50–59, DOI: 10.1109/SASO.2014.17.

[14] Y. Hayashi, “A new design principle of robust onion-like networks self-organized in growth,” Network Science, vol. 6, no. 1, 2018, pp. 54–70, DOI: 10.1017/nws.2017.25.

[15] F. Hu, C. H. Yeung, S. Yang, W. Wang, and A. Zeng, “Recovery of infrastructure networks after localized attacks,” Scientific Reports, vol. 6, no. 2452, 2016, pp. 1–10, DOI: 10.1038/srep24522.

[16] W. Quattrociocchi, G. Caldarelli, and A. Scala, “Self-Healing Networks: Redundancy and Structure,” PLOS ONE, vol. 9, no. 2, 2016, pp. 1–7, DOI: 10.1371/journal.pone.0087986.

[17] M. Stippinger and J. Kertész, “Enhancing resilience of interdependent networks by healing,” Physica A, vol. 416, 2014, pp. 481–487, DOI: 10.1016/j.physa.2014.08.069.

[18] L. K. Gallos and N. H. Fefferman, “Simple and efficient self-healing strategy for damaged complex networks,” Physical Review E, vol. 92, no. 052805, 2015, pp. 1–9, DOI: 10.1103/PhysRevE.92.0528058.

[19] J. Park and S. G. Hahn, “Bypass rewiring and robustness of complex networks,” Physical Review E, vol. 94, no. 022309, 2016, pp. 1–4, DOI: 10.1103/PhysRevE.94.022310.

[20] T. Hayes, N. Rustagi, J. Saia, and A. Trehan, “The Forgiving Tree: A Self-Healing Distributed Data Structure,” in Proceedings of the $27^{th}$ ACM Symposium on Principles of Distributed Computing. ACM NY, USA, Aug. 2008, pp. 203–212, ISBN: 978-1-59593-989-0, DOI: 10.1145/1400751.1400779, URL: https://dl.acm.org/citation.cfm?doid=1400751.1400779 [accessed:2020-03-02].

[21] A. Castañeda, D. Dolev, and A. Trehan, “Compact routing messages in self-healing tree,” Theoretical Computer Science, vol. 709, 2018, pp. 2–19, DOI: 10.1016/j.tcs.2016.11.022.

[22] S. S. Savas, M. F. Habib, M. Tornatore, F. Dikbiyik, and B. Mukherjee, “Network Adaptability to Disaster Disruptions by Exploiting Degraded-Service Tolerance,” IEEE Communications Magazine, vol. 52, 2014, pp. 58–65, DOI: 10.1109/MCOM.2014.6979953, https://ieeexplore.ieee.org/abstract/document/6979953 [accessed:2020-03-02].

[23] Y. Hayashi and N. Uchiyama, “Onion-like networks are both robust and resilient,” Scientific Reports, vol. 8, no. 11241, 2018, pp. 1–13, DOI: 10.1038/s41598-018-29626-w, Author Correction: https://www.nature.com/articles/s41598-018-32563-3 [accessed:2020-03-02].

[24] H.-J. Zhou, “Spin glass approach to the feedback vertex set problem,” Eur. Phys. J. B, vol. 86, no. 445, 2013, pp. 1–9, DOI: 10.1140/epjb/e2013-40690-1.

[25] S. Mugisha and H.-J. Zhou, “Identifying optimal targets of network attack by belief propagation,” Physical Review E, vol. 94, no. 012305, 2016, pp. 1–8, DOI: 10.1103/PhysRevE.94.012305.

[26] Open Flight: http://konect.uni-koblenz.de/networks/opsahl-openflights AS Oregon: http://snap.stanford.edu/data/as.html [accessed:2020-03-02].