Distributed Self-healing under restricted communication: the effect on spatial damages

1st JAEHO KIM
Division of Transdisciplinary Sciences
Japan Advanced Institute of Science and Technology
Nomi, Japan
s2160002@jaist.ac.jp

2nd YUKIO HAYASHI
Division of Transdisciplinary Sciences
Japan Advanced Institute of Science and Technology
Nomi, Japan
yhayashi@jaist.ac.jp

***Keywords*—Self-healing, Robustness of connectivity, Spatially damaged network**

Many infrastructures of communication, transportation, or power-grid systems are represented by a common topological structure called scale-free (SF) [1]. Unfortunately, it is well-known that SF structure is extremely vulnerable against malicious attacks to high degree nodes. Moreover, these weak infrastructures are frequently damaged by natural and man-made disasters. However, the whole connectivity should be perpetually maintained to provide essential services for our daily life.

Therefore, a resilience-based system design has been attracted as an approach to overcome these problems. The concept of resilience includes not only recovering the original structure from disturbances but also reconstructing systems with adaptive capacity [2]. We emphasize that a reconstruction of a damaged network is more important for improving robustness of connectivity. Because, even when infrastructure systems are recovered to original structure, they still have the extremely weak SF structure. Thus, in order to reconstruct a damaged network into more robust one, we have proposed a distributed self-healing method especially based on enhancing loops [3].

The presence of loop structures in a network is a vital factor for the robustness. This is supported by that the network dismantling and decycling problems are asymptotically equivalent in random networks [6]. Here, the dismantling problem is finding the minimum set of nodes which removal makes a network fragmented into at most a given size, while the decycling problem is finding the minimum set of nodes which removal makes all loops from a network. When all loops are removed from a network, the network becomes a tree which is easily fragmented by a removal of few nodes. In other words, for constructing a robust network, it is important to make it hard to become a tree.

Therefore, we have adopted enhancing loops for generating robust structure. In fact, enhancing loops [7], [8] is more effective to generate an onion-like network than other methods such as increasing degree-degree correlations [4], [5]. Here, the onion-like network with positive degree-degree correlations has the optimal robustness against malicious attacks under a given degree distribution [4], [5], in contrast to SF structure.

In the proposed method [3], damaged nodes in a network communicate with other neighboring damaged nodes by exchanging short messages. To maintain a larger connectivity by healing, we assumed that each node of a network has a data set called local map storing identifiers of nodes within three hops from itself. Initially, the local map is defined as a set of candidates nodes for making new connections. Through communicating by some messages, such candidates are extended gradually. After that, damaged nodes which have the same candidates are connected by a ring. Then, the generated ring is enhanced by adding links between low degree nodes on the ring. For the rapid reconstruction, healing links are locally allocated to each node. Thus, it is assumed that nodes reuse some links emanated from attacked nodes. Since the number of reusable links corresponds to a damaged situation, a reusable rate of links is defined by a control parameter r_h which range is $0 < r_h \leq 1$ in our numerical simulation.

The effectiveness of our self-healing has been shown [3] through some investigations for typical infrastructure networks. The reconstructed networks by our method have high robustness against an intentional attack to important nodes with the highest degrees.

However, there is still considerable uncertainty with regard to the effect against other destructive attacks. Therefore, we consider a realistic scenario of disruption caused by spatial disasters. Since a destruction of a real network occurs as removing spatially grouped nodes by earthquakes or floods, we consider Localized Attack (LA) [9] as a malicious attack for reflecting such destruction into infrastructure networks.

In this paper, we have evaluated a network robustness against the attacks: High Degree Adaptive attack (HDA), and LA. HDA is removing highest degree nodes with recalculation of degrees for the networks. A part of connected component as neighbors of a randomly selected node is removed from the networks by LA.

For numerical evaluation of network robustness, we apply the robustness index [4] $R(q) = \frac{1}{N}\sum_{Q=1}^{N} S(Q)(\frac{1}{N} < R(q) \leq 0.5)$ for the reconstructed infrastructure networks after removing qN nodes by HDA, or LA. Here, N is the network size, and $S(Q)$ denotes a ratio of the largest connected component size after removing the number of Q nodes by HDA, or

LA. The index is investigated for the a typical infrastructure network: OpenFlight [10] and AS Oregon [11]. The values of $R(q)$ are averaged over 100 realizations for reconstructed networks.

We show robustness index against two attacks for the networks reconstructed after HDA in Fig.1(a) and (b), or after LA in Fig.1(c) and (d). In particular, we mainly present that the networks reconstructed after one attack also have high robustness against the other attacks.

As shown in each of Fig.1(a) and (c), our method has high values of R_{HDA} after HDA, and R_{LA} after LA. In other words, the reconstructed networks obtain a high robustness against the attack by which they have once been damaged.

Moreover, the reconstructed networks also have high values of robustness against the attack by which they have not been damaged. Fig.1(b) shows the values of $R_{\mathrm{LA}}(q)$ for the networks reconstructed after HDA, and Fig.1(d) shows the values of $R_{\mathrm{HDA}}(q)$ for the networks reconstructed after LA. To be more specific, the networks have the high values of $R_{\mathrm{LA}}(q)$ even for $r_h \leq 0.2$ (red, green, and blue lines in Fig.1(b)). The values of $R_{\mathrm{HDA}}(q)$ are also high especially for $r_h \geq 0.5$ (yellow, and purple lines in Fig.1(d)). However, when $q \geq 0.8$ for highly damaged situations by LA, the values of $R_{\mathrm{HDA}}(q)$ decreases rapidly. The reason of decreasing is considered as follows. Remember that each node can initially communicate with nodes in only three hops from it. Thus, when a huge hole is created by LA in a network, nodes cannot transfer messages to distant nodes. This problem leads to decreasing connectivity in our method. In other words, there is a trade-off between restriction of communication range and maintaining of connectivity. If infrastructures are spatially destroyed over 80%, our method may not work well. However, such highly damaged situations occur very rarely in real life. Even in that situations, it seems to be better not to heal networks but to construct a novel infrastructure. Therefore, we conclude that such trade-off does not become a limitation of our method and that our method is effective against localized attacks.

ACKNOWLEDGMENT

This research is supported in part by JSPS KAKENHI Grant Number JP.21H03425.

REFERENCES

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

[2] C. Folke, Resilience: The emergence of a perspective for social–ecological systems analyses, Global environmental change, 16(3), 253-267, 2006.

[3] J. Kim, and Y. Hayashi, Distributed Self-Healing for Resilient Network Design in Local Resource Allocation Control, Frontiers in Physics, 272, 2022.

[4] C. M. Schneider, A. A. Moreira, J. S. Andrade Jr, S. Havlin, and H. J. Herrmann, Mitigation of malicious attacks on networks, Proceedings of the National Academy of Sciences, 108(10), 3838-3841, 2011.

[5] T. Tanizawa, S. Havlin, and H. E. Stanley, Robustness of onionlike correlated networks against targeted attacks, Physical Review E, 85(4), 046109, 2012.

[6] A. Braunstein, L. Dall'Asta, G. Semerjian, and L. Zdeborová, Network dismantling, Proceedings of the National Academy of Sciences, 113(44), 12368-12373, 2016.

[7] Y. Hayashi, and N. Uchiyama, Onion-like networks are both robust and resilient," Scientific reports, 8(1), 1-13, 2018.

[8] M. Chujyo, and Y. Hayashi, A loop enhancement strategy for network robustness," Applied Network Science, 6(1), 1-13, 2021.

[9] S. Shao, X. Huang, H.E. Stanley, and S. Havlin, Percolation of localized attack on complex networks, New Journal of Physics, 17(2), 023049, 2015.

[10] RA. Rossi, and NK. Ahmed, The network data repository with interactive graph analytics and visualization. AAAI, 2015.

[11] J. Leskovec, J. Kleinberg, and C. Faloutsos, Graphs over time: densification laws, shrinking diameters and possible explanations. Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining, 177–187, 2005.

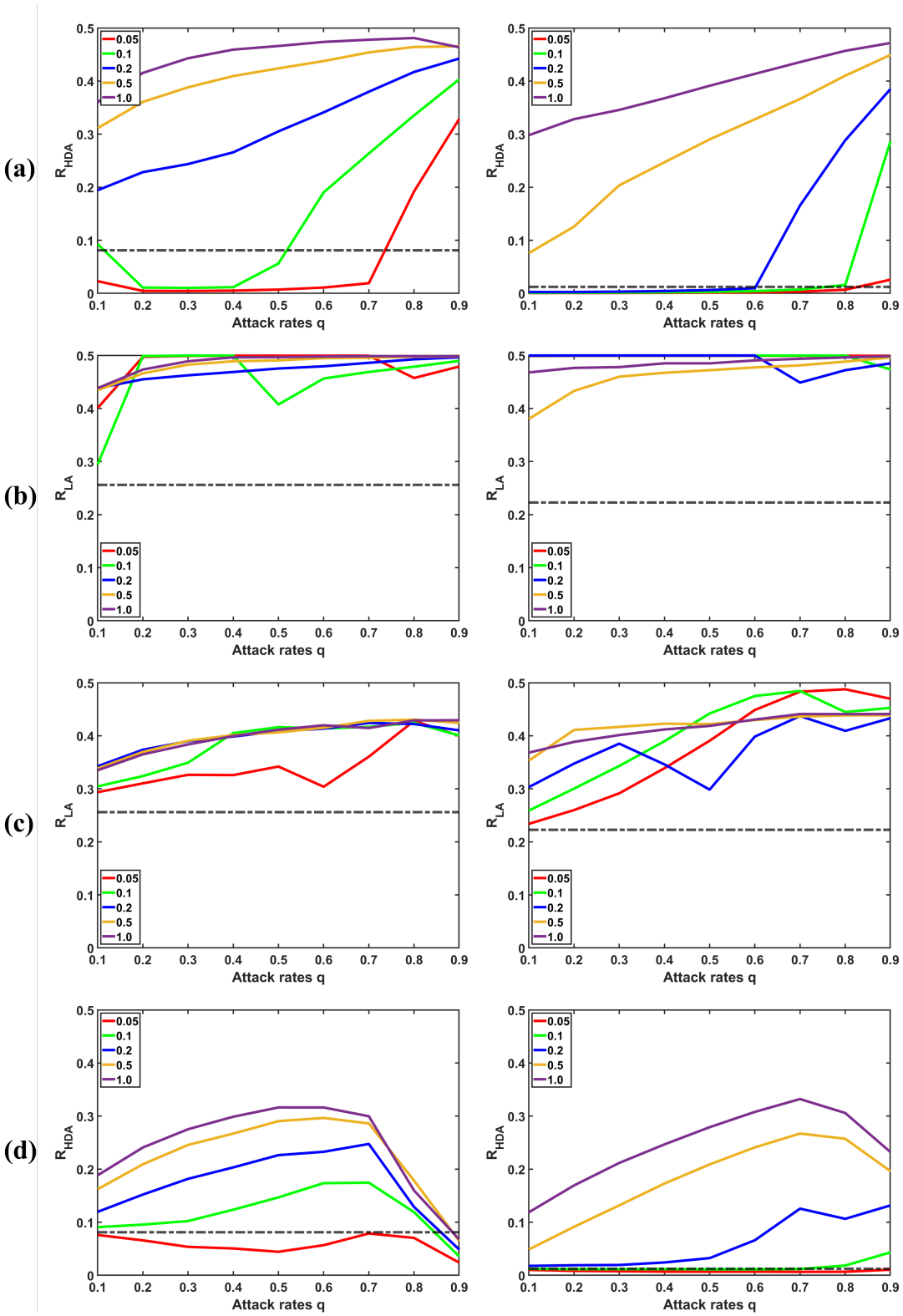

Fig. 1. Robustness of the reconstructed OpenFlight (left column) and AS Oregon (right column). (a) $R_{\mathrm{HDA}}(q)$ for the networks reconstructed after removing qN nodes by HDA. (b) $R_{\mathrm{LA}}(q)$ for them. (c) $R_{\mathrm{LA}}(q)$ for the networks reconstructed after removing qN nodes by LA. (d) $R_{\mathrm{HDA}}(q)$ for them. Colors correspond to several ratio r_h of reused links for healing. Black dot-dash line represents the robustness in the original network as a base-line.