Abstract

Our society is supported by a wide variety of large and complex networks, such as the Internet (WWW), SNS, electric power, transportation, water supply, and international trading systems. These real-world networks commonly have a scale-free property, which is characterized by power-law degree distributions. Unfortunately, scale-free networks are extremely vulnerable against malicious attacks. Thus, it is important to reveal robust networks against attacks and obtain effective methods for strengthening the robustness of the existing networks.

In previous studies, for improving the network robustness of connectivity against attacks, several methods have been proposed so far by enhancing a degree–degree correlation. As a highly robust structure against attacks, an "onion-like structure" with the positive degree–degree correlation have been discussed. Recently, apart from the degree-degree correlation, it has been noticed that the robustness against attacks and loops in networks may be strongly correlated with each other. Therefore, as a new perspective for improving the robustness, we focus on the loops, especially the size of Feedback Vertex Set (FVS), which is the minimum node set whose removal makes the network no loops.

For improving the robustness against attacks, we propose two types of loop-enhancing rewirings, which are expected to increase the size of FVS. We consider two types of rewiring with and without keeping the degree distribution because we also investigate the effect of the degree modification on the robustness. Then, we applied our proposed and conventional methods to some real-world network data and evaluated the improvement in robustness. From the results with keeping degree distributions, our method increases the robustness to the same or more than the state-of-the-art methods based on the degree-degree correlation. In addition, we confirm that our method has the largest increase in the size of FVS. From the results without keeping degree distributions, we find that every our and conventional methods significantly increase both the robustness and the size of FVS, compared to the methods with keeping degree distributions. From these results, the robustness is strongly correlated with the size of FVS more than the conventional degree–degree correlation. Moreover, the modification of degree distributions significantly improves both the robustness and the size of FVS.

As a method for improving the robustness without keeping degree distributions, we investigate link addition methods. In previous studies of link addition methods, two different effective strategies for choosing pairs of unconnected nodes to add links have been considered: the minimum degree and the longest distance strategies. Thus, we propose several kinds of link addition methods with selecting nodes by degree and distance, for investigating the contributions of degrees and distances in improvements of the robustness. Through numerical simulation, the minimum degree strategy is the most effective for improving the robustness in both synthetic and real-world networks. As an exception, only in the small number of added links, the longest distance strategy is the best. Conversely, the shortest distance strategy rarely contributes to improving the robustness, even combined with the minimum degree strategy. Thus, enhancing longer loops is essential for improving the robustness.

Based on the significant increase of the robustness by modifying degree distributions, we investigate robust networks in varying degree distributions. First, we consider the continuously changing degree distributions ranging from power-law to exponential or narrower ones. Numerical results show that the smaller variances of degree distributions lead to higher robustness and the size of FVS in this first range. Second, we consider a random regular graph with the minimum degree variance and the perturbed networks in their comprehensive discrete or random perturbations. In this second range, we find the random regular graphs have the highest robustness against attacks, and find a tendency for smaller degree variance to have higher robustness.

In summary, we emphasize the important points to further improve the robustness against attacks. Enhancing long loops strongly improves the robustness against attacks, more than the conventional degree-degree correlation. For adding links, the minimum degree strategy is the most effective for improving the robustness. We suggest that the random regular graph with the minimum degree variance has optimal robustness.

keywords: Network robustness against attacks, Enhancing loops, Link addition methods, The minimum degree strategy, The minimum variance of degree distributions.