2015 International Symposium on Nonlinear Theory and its Applications
NOLTA2015, Kowloon, Hong Kong, China, December 1-4, 2015

Synchronizability and Attack Optimization of Dynamical Scale-free Networks

Shiwen Sun†, Yilin Ma‡, Ruiqi Li‡, Li Wang† and Chengyi Xia†

†Tianjin Key Laboratory of Intelligence Computing and Novel Software Technology,
Tianjin University of Technology, Tianjin, 300384, P. R. China
‡School of Computer and Communication Engineering, Tianjin University of Technology,
Tianjin, 300384, P. R. China
Email: sunsw80@126.com

Abstract—Recently, an effective network optimization method was introduced to improve the ability to resist malicious attacks and the optimized networks have an typical onion-like structure. So far, the study on onion-like networks mainly focused on their structural properties and the enhancement of attack robustness. However, in our paper, we investigate one aspect of dynamical processes in complex networks, namely synchronization behavior. Through extensive numerical simulations, it is found that solely enhancing the network robustness can lead to the reduction of the ability to achieve synchronization. Current results are beneficial for us to deeply understand the dynamical properties and patterns in the complex networked systems.

1. Introduction

Many real-world complex systems can be characterized and analyzed by networks or graphs with complex topologies [1, 2]. Especially, in the past decade many theoretical and experimental works have been performed to analyze the attack robustness of a vast variety of different networked systems. Albert et al. [3] found the "*robust yet fragile*" generic property of scale-free networks: scale-free networks display an unexpected degree of robustness to random failure; however, they are extremely vulnerable to intentional attacks. This work has triggered successively enormous interest on the effect of different topological properties on the attack robustness of networks, including the degree distribution, centrality, assortativity, the interaction strength of the edges and so on [4, 5, 6]. Meanwhile, many researchers also have devoted a great deal of efforts to the study of how to construct optimal networks and how to make existing networks more robust against random and/or targeted attacks [7].

In a recent work [8], Schneider et al. propose a new measure for network robustness under malicious attacks on highly connected nodes. For an existing network with a prescribed degree distribution, based on a simple greedy algorithm, they also present an link-rewiring method which can significantly improve the robustness. It has been discovered that independent of the degree distributions of the networks, the most robust structures exhibit an "onion-like" topology in which high-degree nodes form a core surrounded by rings of nodes with decreasing degree [9]. However, although it is proved that this optimization method is effective in increasing the robustness of networks against malicious attacks, would the structural adjustment affect other dynamical behaviors occurring in networks? That is the motivation of our following study. In this paper we study one aspect of dynamical behaviors in complex networks, namely synchronization. Synchronization is the mechanism responsible for numerous phenomena in natural world and modern society, which has attracted a lot of research efforts [10].

The rest of the paper is organized as follows. In section 2, the novel quantity R used to evaluate network's resilience resisting malicious attacks is presented. After that, the general framework for synchronization stability of coupled dynamical systems is briefly discussed. In section 3, numerical simulations are performed to analyze the the relationship between the robustness and the synchronizability of scale-free networks; moreover, the change of synchronizability during optimization process is investigated. Finally we conclude the whole paper in the last section.

2. Models

2.1. Dynamical network model and the stability criteria for synchronization

Consider a dynamical network consisting of N coupled identical nodes, with each node being an n-dimensional dynamical system, whose state equation can be described by

$$\dot{x}_i = f(x_i) - c\sum_{j=1}^{N} a_{ij}H(x_j), \qquad i = 1, 2, \ldots, N, \quad (1)$$

where $f(\cdot)$ is a given nonlinear function, $x_i = (x_{i1}, x_{i2}, \ldots, x_{in}) \in \mathbb{R}^n$ are the state variables of node i, $c > 0$ is the coupling strength. $H(\cdot) : \mathbb{R}^n \to \mathbb{R}^n$ is called the *inner linking function*. $A = \{a_{ij}\}_{N\times N}$, which is called the *topological matrix*, represents the coupling configuration of the underlying network. Only considering symmetric and diffusive coupling, A is a Laplacian matrix. For a connected network, A is irreducible, 0 is an eigenvalue of A with multiplicity 1, and all the other eigenvalues are strictly positive, i.e. $0 = \lambda_1 < \lambda_2 \leq \cdots \leq \lambda_N$.

The dynamical network (1) is said to be (asymptotically) *synchronized*if $x_1(t) = x_2(t) = \cdots = x_N(t) \to s(t), t \to$

∞ [11]. In addition, according to the shape of synchronized region $S \subseteq R$, dynamical networks can be divided into several types:

(i) **Type I networks** with an unbounded synchronized region $S \in (-\infty, \alpha_2]$, $\alpha_2 < 0$: the eigenvalue λ_2 of A determines the synchronizability, the larger the λ_2, the easier the synchronization is, and vice visa [11];

(ii) **Type II networks** with a bounded synchronized region $S \in [\alpha_1, \alpha_2]$,$-\infty < \alpha_1 < \alpha_2 < 0$: a larger value of the ratio λ_N/λ_2 corresponds to poor synchronizability, and vice versa [12];

(iii) dynamical networks with $S = \phi$, the coupled system can not achieve any synchronization.

2.2. Optimized network model

Recently, Schneider et al.[8] proposed a novel measure, node robustness R, to evaluate the robustness of networks under attacks considering the size of the largest connected component during all possible malicious attacks, namely

$$R = \frac{1}{N}\sum_{q=1}^{N-1} S(q), \tag{2}$$

where N is the total number of nodes in the initial network and $S(q)$ denotes the relative size of the largest connected component after removing q nodes with the highest degrees. Generally, the larger the value of R, the more robust the network resisting intentional attacks on high degree nodes.

With the robustness criterion R in mind, the network optimization problem can be defined as follows: given a network G with the predefined degree distribution $p(k)$, how to maximize R while keeping both the degree distribution and the degree of every node unchanged. Based on greedy algorithm, an edge-swap method was developed to improve network robustness resisting intentional attacks, while keeping the degrees of per node invariant and the whole network connected. A simple example is shown in Fig. 1.

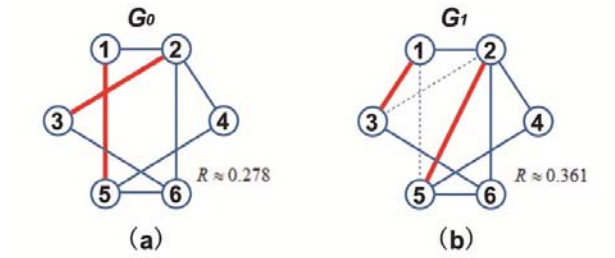


Figure 1: Demonstration of edge-swap in a network. The initial network G_0 (a) is with $N = 6$ nodes, $L = 8$ edges and $R_0 \approx 0.278$. After performing the swap on edges (i.e. edges $(1, 5)$ and $(2, 3)$ to new edges $(1, 3)$ and $(2, 5)$), the resultant network G_1 (b) gets an improved R value, $R_1 = 0.361$.

3. Numerical simulation and analysis

3.1. Robustness measure R of scale-free networks

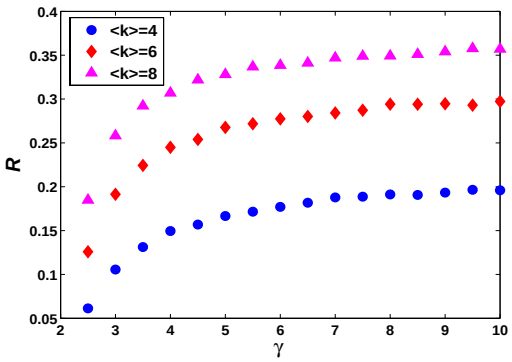


Figure 2: The values of robustness measure R of scale-free networks with $N = 1000$ and $\langle k\rangle = 4(\bullet), 6(\blacklozenge), 8(\blacktriangle)$ for different scaling exponents γ.

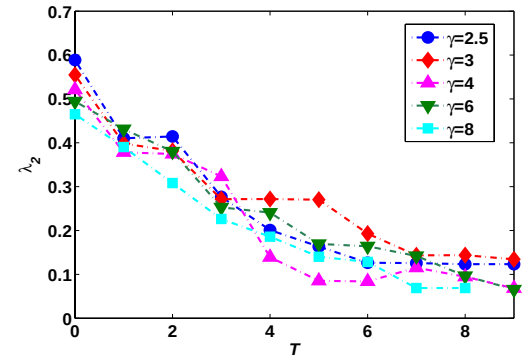
It can be observed from Fig. 2 that, R increases as the scaling exponent γ becomes larger, which indicates that scale-free networks with larger γ are more robust to resist malicious attacks and vice versa. For all the power-law distributions, a smaller γ corresponds to a broader distribution, thus corresponding network becomes more heterogenous in connectivity. Consequently, for scale-free networks with fixed number of nodes and links, the smaller the value of γ, the more vulnerable the network resisting malicious attacks on hub nodes.

Furthermore, scale-free networks with fixed exponent are examined. As $\langle k\rangle$ becomes larger, R is observed to increase(see Fig. 2), which indicates that scale-free networks with larger $\langle k\rangle$ have higher ability to resist attacks. A larger $\langle k\rangle$ indicates that more links exist in the network, thus leading to the increase of the extent of alternative path redundancy between nodes and improved invulnerability of the whole network.

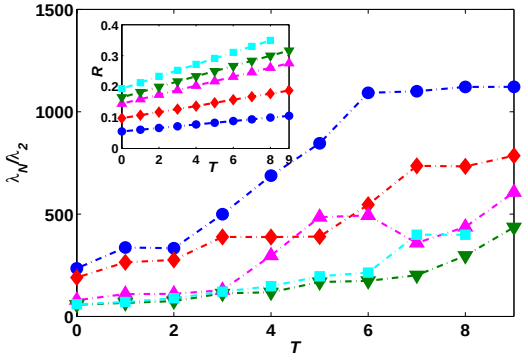
3.2. Synchronizability of optimized scale-free networks

It can be concluded that the impact of a particular coupling topology on the system's ability to synchronize can be characterized by the following quantities: λ_2 for **Type I** and λ_N/λ_2 for **Type II networks**. Now we will investigate the change of the synchronizability of dynamical systems with scale-free structures before and after the optimization mentioned above. The inset of Fig. 3(b) presents the optimization results of scale-free networks with $N = 1000$, $\langle k\rangle = 4$ and different γ. At each step T, with several edge swaps, a 20% increase of R is recorded. Thus the R of resultant network after optimization is almost twice as much as the initial value.

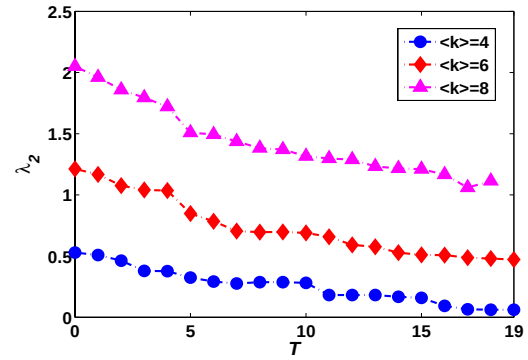
In order to explore the stability of synchronization of optimized networks, the eigenvalues of corresponding net-



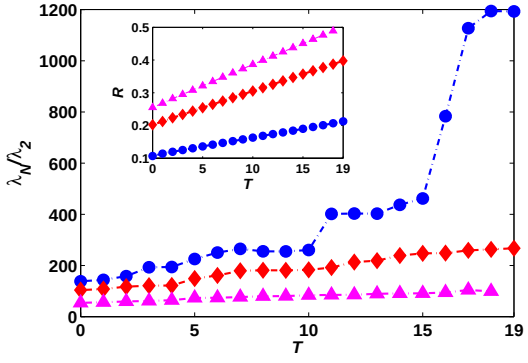
(a)



(b)



(c)



(d)

Figure 3: The eigenvalues λ_2(a) and λ_N/λ_2(b) of dynamical scale-free networks during optimization.

works are obtained numerically and the behaviors with the optimization step T are exhibited in Fig. 3. It can be found that λ_2 (Fig. 3(a)) becomes smaller and the ratio λ_N/λ_2 (Fig. 3(b)) becomes larger with step T, which strongly demonstrates that, for both Type I and Type II dynamical systems the optimized networks with improved R have poorer stability to achieve synchronization.

Furthermore, dynamical scale-free networks with fixed N and γ for different $\langle k\rangle$ are also investigated (see Fig. 3(c) and Fig. 3(d)). The inset of Fig. 3(d) displays the optimization results of scale-free networks with $N = 1000$, $\gamma = 3$ and $\langle k\rangle = 4(\bullet), 6(\blacklozenge), 8(\blacktriangle)$. At each optimization step T, a 10% increase of R is recorded. Thus after optimization($T = 19$), the resultant networks have doubled R values comparing to the initial networks. The eigenvalues which measures the ability to achieve synchronization of dynamical scale-free networks are exhibited in Fig. 3(c) and Fig. 3(d). Clearly, with the optimization step T, the eigenvalue λ_2 is observed to decease(Fig. 3(c)),and λ_N/λ_2 is observed to increase(Fig. 3(d)), which implies the reduced synchronizability during optimization.

3.3. Discussion

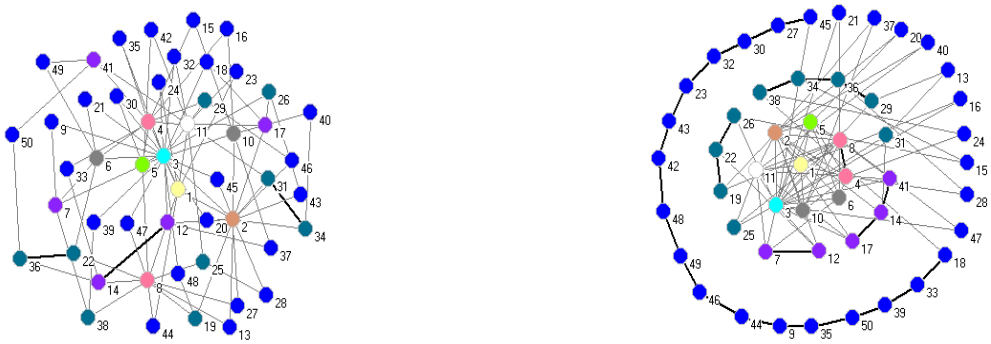
Noticeably, during network optimization the link-rewiring method keeps the degree of every node unchanged while improving the robustness. In other words, networks have the same degree distribution before and after the optimization. Previous study has investigated the effect of degree distribution and degree heterogeneity on the synchronization behaviors of dynamical networks [10]. However, our findings demonstrate that the degree heterogeneity of underlying topology has no direct relationship with the ability to achieve synchronization.

As shown in Fig. 4, optimized network exhibits a type of "onion-like" topology, i.e. a core composed of high-degree hub nodes exists which is hierarchically surrounded by rings of nodes with decreasing degree. Previous study has shown that node load can be regarded as a suitable predictor for the synchronizability on complex dynamical networks [13]. Since many paths pass through the "center" nodes, they tend to get overloaded, consequentially leading to the loss of the synchronized state information to be exchanged between dynamical nodes.

4. Conclusions

By utilizing a recently introduced optimization method, scale-free networks can be optimized with increased ability to resist malicious attacks. In our study, firstly, we examined the relationship between the node robustness measure R and two important topological parameters: the scaling exponent γ and the average node degree $\langle k\rangle$.

Next, we explored how the synchronization is affected by the optimization aiming at increasing the robustness against attacks. Large quantities of numerical results veri-



(a) (b)

Figure 4: Visualization of network topologies of a scale-free network before and after optimization. The networks are with size $N = 50$, average node degree $\langle k \rangle = 4$ and degree distribution $p(k) \sim k^{-3}$. Nodes with similar degree have the same color. Edges between nodes with equal degree are highlighted with bold black lines. (a) initial network with $R = 0.1404$; (b) onion-like topology of optimized network with enhanced $R = 0.3828$.

fied that, for both Type I and Type II dynamical systems, the synchronizability of optimized scale-free networks is suppressed as R is increased. Thus, our findings strongly demonstrate that a special attention should be paid to the tradeoff between maximizing the attack robustness and improving the synchronizability in system design. These results can provide insights into deeply understanding the dynamical properties of large-scale complex networked systems.

Acknowledgments

This work was partially supported by the National Natural Science Foundation of China under Grant Nos. 61203138, 61403280 and 61374169. SWS and CYX acknowledge the support from "131" Innovative Talents Program of Tianjin.

References

[1] R. Albert, A.L. Barabási, "Statistical mechanics of complex networks," *Rev. Mod. Phys.*, vol.74, pp.47-97, 2002.

[2] M.E.J. Newman, "The structure and function of complex networks," *SIAM Review*, vol.45(2), pp.167-256, 2003.

[3] R. Albert, H. Jeong, A.L. Barabási, "The Internets Achilles Heel: error and attack tolerance of complex networks," *Nature*, vol.406, pp.378-382, 2000.

[4] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, "Resilience of the Internet to random breakdowns," *Phys. Rev. Lett.*, vol.85(21), pp.4626-4628, 2000.

[5] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin. "Breakdown of the Internet under intentional attack," Phys. Rev. Lett., vol.86(16), pp.3682-3685, 2001.

[6] D.S. Callaway, M.E.J. Newmann, S.H. Strogatz, D.J. Watts, "Network robustness and fragility: percolation on Random Graphs," *Phys. Rev. Lett.*, vol.85(25), pp.5468-5471, 2000.

[7] G. Paul, S. Sreenivasan, S. Harlin, H.E. Stanley, "Optimization of network robustness to random breakdowns," *Physica A*, vol.370(2), pp.854-862, 2006.

[8] C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, "Mitigation of malicious attacks on networks," *PNAS*, vol.108(10), pp.3838C3841, 2011.

[9] Z.X. Wu, P. Holme, "Onion structure and network robustness," *Phys. Rev. E*, vol.84, pp.026106, 2011.

[10] A. Arenas, A. Diaz-Guilera, J.Kurths, Y. Moreno, C. Zhou, "Synchronization in complex networks," *Phys. Rep.*, vol.469, pp.93-153, 2008.

[11] X.F. Wang, G. Chen, "Synchronization in scale-free dynamical networks: robustness and fragility," *IEEE T. CIRCUITS-I*, vol.49(1), pp.54-62, 2002.

[12] L.M. Pecora, T.L. Carroll, "Master stability functions for synchronized coupled systems," *Phys. Rev. Lett.*, vol.80, pp.2109-2112, 1998.

[13] T. Nishikawa, A.E. Motter, Y.C. Lai, "Heterogeneity in oscillator networks: are smaller worlds easier to synchronize?" *Phys. Rev. Lett.*, vol.91(1), pp.014101, 2003.