2016 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2016, Yugawara, Japan, November 27th-30th, 2016

Theory for Dynamical Robustness of Complex Networks against Targeted Attacks

Tianyu Yuan†, Kazuyuki Aihara†,‡, Gouhei Tanaka†,‡

†Department of Electrical Engineering and Information Systems, the University of Tokyo,
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
‡Institute of Industrial Science, the University of Tokyo,
4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Japan
Email: yty@sat.t.u-tokyo.ac.jp, aihara@sat.t.u-tokyo.ac.jp, gouhei@sat.t.u-tokyo.ac.jp

Abstract– Many real-world networks do not have simple static structures but dynamics on them, such as many social, biological and computer networks. Such networks are heterogeneously connected. It is meaningful to investigate the dynamical robustness of complex networks against random failures and targeted attacks. So far the theory for analyzing the dynamical robustness against random failures has been developed, but that against targeted attacks is missing. This paper derives an analytical expression for the critical value which measures the dynamical robustness against targeted attacks for a general kind of coupled dynamical networks.

1. Introduction

Real-world networks are often heterogeneous, which have a wide range of degree distribution. One famous case is the scale-free network with power law degree distribution [1]. Such networks are known to be robust against random failures but very fragile to targeted attacks at hubs [2], which means preferential removal of high-degree nodes. This is the result of the analysis in the framework of structural robustness where only connectivity of the networks governs the robustness. The theoretical treatment has been based on the percolation theory [3, 4, 14]. However, it is also necessary to study dynamical robustness of complex networks, which is especially important in biological phenomena because the function of biological networks is usually considered to depend on both structure and dynamics [5].

In this paper we deal with dynamical robustness of diffusively coupled oscillator networks with complex topology. The dynamical robustness represents how the dynamical behavior in the whole network is tolerant against local failures. In the dynamical robustness framework, the local failures correspond to inactivation of the oscillator nodes. The fraction of the inactivated nodes is denoted by p. The order parameter is introduced to measure the level of the oscillatory behavior in the whole network and the critical inactivation ratio p_c, at which a loss of oscillatory dynamics (aging transition [6]) occurs, is used to measure the network robustness. This framework for study of oscillator networks has been first introduced for globally coupled networks in Ref. [6] and subsequently extended to complex networks [7-11]. These studies have employed the Stuart-Landau oscillators which generate oscillations via the Hopf bifurcation. The most striking result of the dynamical robustness analysis is that the oscillator network can be highly fragile to the attack targeted at low-degree oscillator nodes, instead of high-degree hub nodes [7]. The critical value p_c has been analytically obtained for random failures [7], but not for targeted attacks. The main work of this paper is to give the theoretical p_c for targeted attacks, which works for a general diffusively coupled oscillators including the Stuart-Landau model. It is shown analytically that the property of dynamical robustness is different from the structural robustness, indicating that the effects of high-degree attack, low-degree attack, and random failures depend on the range of parameters.

2. Methods

We consider a general kind of diffusively coupled oscillators as below:

$$\dot{z}_j = F(z_j) + h_j \sum_{k=1}^{N} A_{jk}(z_k - z_j), \quad \text{for } j = 1, \dots, N, \tag{1}$$

where $F(z_j)$ is the function representing the dynamics of individual nodes, exhibiting a bifurcation; N is the number of oscillators; z_j is the complex value representing the state of the jth oscillator; A_{jk} is the adjacency matrix which takes any real value and does not have to be symmetric; h_j is a tuning term. If h_j depends on $A_j = \sum_{k=1}^{N} A_{jk}$, then it becomes a weighted network, which is studied in Ref. [8]. Although z_j is supposed to be complex, we assume based on numerical observation that all nodes tend to have the identical phases, so z_j can be viewed as real.

A widely used special case is described as follows [6]:

$$\dot{z}_j = \left(\alpha_j + i\Omega - |z_j|^2\right) z_j + \frac{K}{N}\sum_{k=1}^{N} A_{jk}(z_k - z_j), \quad \text{for } j = 1, \dots, N, \tag{2}$$

where Ω is the natural frequency; K is the coupling strength. Here A_{jk} takes the value of 0 or 1. Later we will consider model (2) as well as a weighted coupling case described as follows [8]:

$$\dot{z}_j = \left(\alpha_j + i\Omega - |z_j|^2\right) z_j + \frac{K\langle k\rangle}{Nk_j}\sum_{k=1}^{N} A_{jk}(z_k - z_j),$$
$$\text{for } j = 1, \dots, N, \quad (3)$$
where $k_j = \sum_{k=1}^{N} A_{jk}$ is the degree of the jth node and $\langle k\rangle$ is the average degree. An isolated oscillator (K=0) is called the Stuart-Landau oscillator, which represents the normal form of Hopf bifurcation which occurs at $\alpha_j = 0$. An oscillator is called active when $\alpha_j = a > 0$ and inactive when $\alpha_j = -b < 0$. An inactive oscillator tends to approach the origin with $|z_j| = 0$ after transient damped oscillations while an active oscillator tends to the limit cycle with amplitude $|z_j| = \sqrt{a}$. Such notations can also be used for the general case (1): an active oscillator with $F(z_j) = F_A(z_j)$ and an inactive one with $F(z_j) = F_I(z_j)$. Therefore random failures and targeted attacks can be defined as inactivation of active oscillators.

The order parameter $|Z|$ is defined to measure the level of oscillation of the network: $|Z| \coloneqq \frac{1}{N}\sum_{j=1}^{N} z_j$. As the ratio p of inactive oscillators increases from 0 to 1, the order parameter $|Z|$ decreases and will reach 0 at some critical ratio p_c. We can use p_c as a measure of dynamical robustness. To calculate the critical ratio p_c, we assume the heterogeneous (degree-weighted) mean field approximation [7, 12]. Moreover we remove the phase rotation of all nodes and assume that every z_j is real. Let $A_j = \sum_{k=1}^{N} A_{jk}$ and then

$$H_A(t) = \sum_{j\in S_A} A_j z_j(t), H_I(t) = \sum_{j\in S_I} A_j z_j(t), \quad (4)$$

where S_A and S_I are the sets of active and inactive nodes, respectively. Then the mean-field approximation gives

$$\sum_{k=1}^{N} A_{jk} z_k \cong A_j \frac{\sum_k A_k z_k(t)}{\sum_k A_k} = A_j \frac{H_A(t)+H_I(t)}{\sum_k A_k}. \quad (5)$$

This equation assumes that every link connects to any node with the same probability, i.e. the network is uncorrelated. By substituting Eq. (5) into Eq. (1) and considering the condition for an equilibrium, we obtain

$$\dot{z}_j = f(z_j, H_A, H_I)$$
$$= F(z_j) + h_j A_j \left(\frac{H_A(t) + H_I(t)}{\sum_k A_k} - z_j\right) = 0.$$

Then, it follows

$$\frac{\partial z_j}{\partial H_I} = \frac{\partial z_j}{\partial H_A} = -\frac{\frac{\partial f}{\partial H_A}}{\frac{\partial f}{\partial z_j}} = \frac{\frac{h_j A_j}{\sum_k A_k}}{h_j A_j - \frac{\partial F}{\partial z_j}}, \quad (6)$$

where $F(z_j) = \begin{cases} F_A(z_j) & \text{for active nodes} \\ F_I(z_j) & \text{for inactive nodes} \end{cases}.$

The derivative of Eq. (4) to $H_A(t)$, $H_A(t)$ becomes

$$J = \begin{bmatrix} \frac{\partial}{\partial H_A}(\sum_{j\in S_A} A_j z_j(t)) - 1 & \frac{\partial}{\partial H_I}(\sum_{j\in S_A} A_j z_j(t)) \\ \frac{\partial}{\partial H_A}(\sum_{j\in S_I} A_j z_j(t)) & \frac{\partial}{\partial H_I}(\sum_{j\in S_I} A_j z_j(t)) - 1 \end{bmatrix}. \quad (7)$$

From the inverse function theorem, (4) has a derivable solution if and only if J is nonsingular. It is easy to see that the condition corresponds to the case when the network is still active. Therefore at the critical ratio p_c, J is supposed to be singular: $det(J)|_{H_A=H_I=0} = 0$, and thus we get the equations below:

$$\sum_{j=1}^{N} A_j = \sum_{j\in S_I} \frac{h_j A_j^2}{h_j A_j - \dot{F}_I(0)} + \sum_{j\in S_A} \frac{h_j A_j^2}{h_j A_j - \dot{F}_A(0)}. \quad (8)$$

For random failures, Eq. (8) becomes

$$\sum_{j=1}^{N} A_j = p_c \sum_{j=1}^{N} \frac{h_j A_j^2}{h_j A_j - \dot{F}_I(0)} + (1 - p_c)\sum_{j=1}^{N} \frac{h_j A_j^2}{h_j A_j - \dot{F}_A(0)}, \quad (9)$$

and thus

$$p_c = \frac{\sum_{j=1}^{N} \frac{h_j A_j^2}{h_j A_j - \dot{F}_A(0)} - \sum_{j=1}^{N} A_j}{\sum_{j=1}^{N} \frac{h_j A_j^2}{h_j A_j - \dot{F}_A(0)} - \sum_{j=1}^{N} \frac{h_j A_j^2}{h_j A_j - \dot{F}_I(0)}}. \quad (10)$$

For targeted attacks, we sort the indices of oscillators by the preferential order of attacks, and thus the oscillators $j = 1, \dots, Np_c$ are inactive and $j = Np_c + 1, \dots, N$ are active. Since the right-hand side if Eq. (8) is supposed to be a monotone function of p_c, there has to be a solution p_c satisfying the following equation.

$$\sum_{j=1}^{N} A_j = \sum_{j=1}^{Np_c} \frac{h_j A_j^2}{h_j A_j - \dot{F}_I(0)} + \sum_{j=Np_c+1}^{N} \frac{h_j A_j^2}{h_j A_j - \dot{F}_A(0)}. \quad (11)$$

The solution p_c is numerically found in practice.

For the coupled Stuart-Landau oscillator model in Eq. (2), the expressions become as below:

For random failures:

$$p_c = \frac{\sum_{j=1}^{N} \frac{k_j^2}{k_j - aN/K} - \sum_{j=1}^{N} k_j}{\sum_{j=1}^{N} \frac{k_j^2}{k_j - aN/K} - \sum_{j=1}^{N} \frac{k_j^2}{k_j + bN/K}}. \quad (12)$$

This formula is consistent with the previous result [7].

For targeted attacks:

$$\sum_{j=1}^{N} k_j = \sum_{j=1}^{Np_c} \frac{k_j^2}{k_j + bN/K} + \sum_{j=Np_c+1}^{N} \frac{k_j^2}{k_j - aN/K}. \quad (13)$$

For the weighted coupling model in Eq. (3), it turns out to be very simple:

For random failures:

$$p_c = \frac{1 + \frac{bN}{K\langle k\rangle}}{1 + \frac{b}{a}}. \quad (14)$$

For targeted attacks:

$$N = \frac{1}{\langle k\rangle + bN/K}\sum_{j=1}^{Np_c} k_j + \frac{1}{\langle k\rangle - aN/K}\sum_{j=Np_c+1}^{N} k_j. \quad (15)$$

Obviously in the case of weighted coupling networks the low-degree attack always gives the higher p_c and the high-degree attack gives the lower p_c.

3. Results

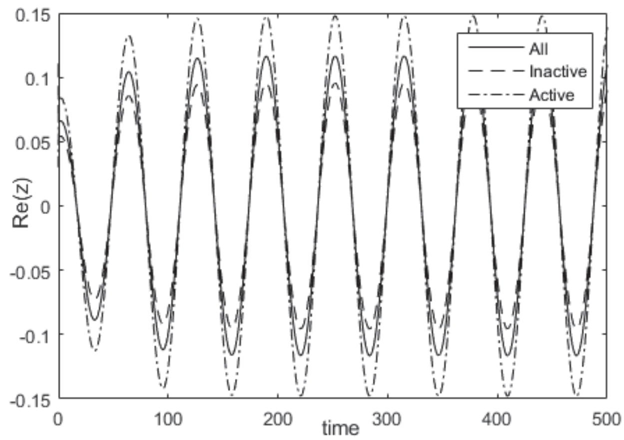
In this section we show that the theoretically derived p_c is valid in numerical simulations for the Stuart-Landau model and the weighted coupling Stuart-Landau model. Numerical computation is run by the Matlab's built-in function ode45, a four-five order Runge-Kutta method. All results are sampled after running 1000 time steps. For targeted attacks we consider the special cases of attacks targeted at the high-degree nodes (high-degree attack) and at the low-degree nodes (low-degree attack). Therefore the sorting of attack preference is just sorting by degrees.

Figure 1(a) shows the time courses of the oscillatory dynamics after a sufficiently long time, for the whole oscillators, the active group, and the inactive group. Each curve represents the real part of the state variables averaged over each group. The mean value of all oscillators gets stable at time 500. Figure 1(b) shows the procedure of the aging transition for a randomly connected network. The behavior of the curve near p_c is studied in Ref. [6]. In this case, the network is more vulnerable to the low-degree attack than to the high-degree attack.

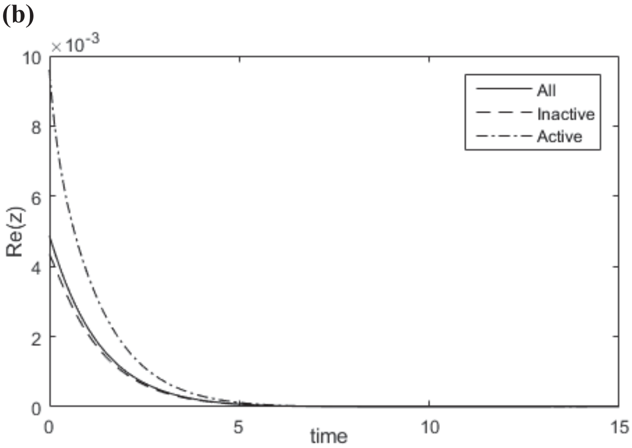
Figure 2 shows the critical ratio p_c vs coupling strength *K*. The numerical results match well with the theoretically computed p_c. In Fig. 2(a), the low-degree attack leads to the smaller p_c compared with the random failure and the high-degree attack for the whole range of *K*. However, this property does not hold when the parameter values of *a* and *b* are changed. From Eq. (13), it is easy to see that when *a* is very small, the high-degree attacks will finally have lower p_c, as shown in Fig. 2(b) with *a*=0.1 and *b*=1.

Figure 3 shows the weighted coupling case. As predicted by Eq. (15), the high-degree attack gives the lowest p_c while the low-degree attack gives the highest, which matches the result in [8].

(a)



(b)



(c)

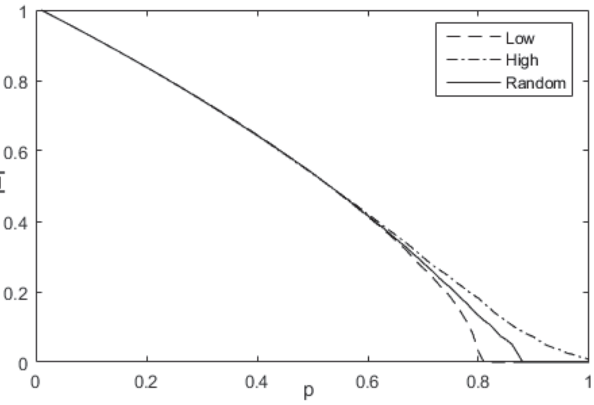
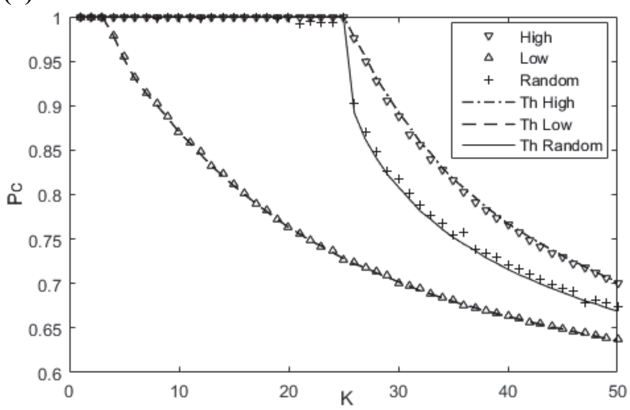


Figure 1. (a)(b) Mean values of oscillators vs time for different *p*. (a) is the case of random failure at *p*=0.6, (b) is the damped case of random failure at *p*=0.9. (c) The order parameter $|Z|$ vs inactivation ratio *p*. The parameters are set at *N*=100, connection density *d*=0.3*, a*=*b*=1*, Ω*=0.1, and *K*=5.

(a)



(b)

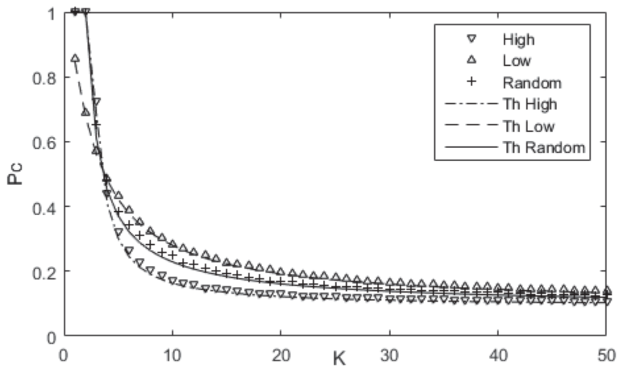


Figure 2. The critical ratio p_c vs the coupling strength *K*. The number of oscillators is *N*=1000; the scale-free network is built by Barabási–Albert method with preferential attachment of 40 links each step. Ω=0.1. (a) *a*=*b*=1; (b) *a*=0.1, *b*=1.

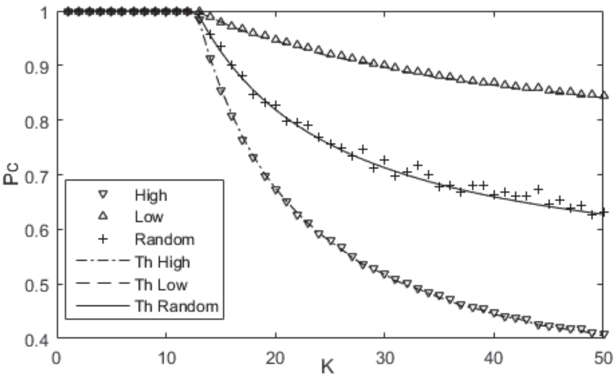


Figure 3. The critical ratio p_c vs the coupling strength *K* for the weighted network. The number of oscillators is *N*=1000; the scale-free network is built by Barabási–Albert method with preferential attachment of 40 links each step. Ω=0.1. (a) *a*=*b*=1; (b) *a*=0.1, *b*=1.

4. Conclusions

In this study, we have derived the theoretical formula for the critical value of p_c for targeted attacks in a general network model of diffusively coupled bifurcating systems. The theoretical results are in good agreement with the numerical ones in the scale-free networks of coupled Stuart-Landau oscillators and the weighted coupling model. It has been demonstrated that the attack method which is most dangerous for network robustness can change depending on the dynamics of the individual components of the network.

The theoretically derived critical values in Eqs. (9)-(10) are not confined to these cases and should work for other types of targeted attacks. However, the computation of the critical ratio requires the mean-field approximation, thus the theoretical p_c may be problematic for networks with high-order connection, such as correlated networks [13]. Since the theoretical p_c only depends on the degree distribution and attack preference, it has no high-order information of the network.

Future works will consider other types of dynamical components as well as different preferential attacks. Moreover, it is worth extending the study to correlated networks and pulse-coupled networks.

References

[1] Barabási A L, Albert R. Emergence of scaling in random networks. Science, 1999, 286(5439): 509-512.
[2] Albert R, Jeong H, Barabási A L. Error and attack tolerance of complex networks. Nature, 2000, 406(6794): 378-382.
[3] Callaway D S, Newman M E J, Strogatz S H, et al. Network robustness and fragility: Percolation on random graphs. Physical Review Letters, 2000, 85(25): 5468.
[4] Cohen R, Erez K, Ben-Avraham D, et al. Resilience of the Internet to random breakdowns Physical Review Letters, 2000, 85(21): 4626.
[5] Barabási A L, Oltvai Z N. Network biology: understanding the cell's functional organization. Nature Reviews Genetics, 2004, 5(2): 101-113.
[6] Daido H, Nakanishi K. Aging transition and universal scaling in oscillator networks. Physical Review Letters, 2004, 93(10): 104101.
[7] Tanaka G, Morino K, Aihara K. Dynamical robustness in complex networks: the crucial role of low-degree nodes. Scientific Reports, 2012, 2:232.
[8] He Z, Liu S, Zhan M. Dynamical robustness analysis of weighted complex networks. Physica A: Statistical Mechanics and its Applications, 2013, 392(18): 4181-4191.
[9] Tanaka G, Morino K, Daido H, et al. Dynamical robustness of coupled heterogeneous oscillators. Physical Review E, 2014, 89(5): 052906.
[10] Huang W, Zhang X, Hu X, et al. Variation of critical point of aging transition in a networked oscillators system. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2014, 24(2): 023122.
[11] Tanaka G, Morino K, Aihara K. Dynamical robustness of complex biological networks. Mathematical Approaches to Biological Systems. Springer Japan, 2015: 29-53.
[12] Pastor-Satorras R, Vázquez A, Vespignani A. Dynamical and correlation properties of the Internet. Physical Review Letters, 2001, 87(25): 258701.
[13] Sasai T, Morino K, Tanaka G, et al. Robustness of Oscillatory Behavior in Correlated Networks. PLOS ONE, 2015, 10(4): e0123722.
[14] Cohen R, Erez K, Ben-Avraham D, et al. Breakdown of the Internet under intentional attack. Physical Review Letters, 2001, 86(16): 3682.