Physica A 394 (2014) 370–378

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Analysis of percolation behaviors of clustered networks with partial support–dependence relations

Gaogao Dong [a,b,*], Lixin Tian [a], Ruijin Du [a,b], Min Fu [a], H. Eugene Stanley [b]

[a] Nonlinear Scientific Research Center, Faculty of Science, Jiangsu University, Zhenjiang, 212013, China

[b] Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA

HIGHLIGHTS

- The robustness of clustered networks with partial support–dependence relations is studied by adopting two attack strategies.
- The first order region becomes smaller as average degree or clustering coefficient increases.
- The second order region becomes larger as average degree or clustering coefficient increases.
- Clustering coefficient has a significant impact on robustness of the system for strong coupling strength.
- For weak coupling strength, clustering coefficient has little influence, especially for attacking both networks.

ARTICLE INFO

Article history:
Received 24 July 2013
Received in revised form 30 August 2013
Available online 7 October 2013

Keywords:
Clustered networks
Robustness
Interdependent network

ABSTRACT

We carry out a study of percolation behaviors of clustered networks with partial support–dependence relations by adopting two different attacking strategies, attacking only one network and both networks, which help to further understand real coupled networks. For two different attacking strategies we find that the system changes from a second-order phase transition to a first-order phase transition as coupling strength q increases. We also notice that the first-order region becomes smaller and the second-order region becomes larger as average degree or clustering coefficient increases. And, as the average supported degree approaches infinity, coupled clustered networks become independent and only the second-order transition is observed, which is similar to $q = 0$. Furthermore, we find that clustering coefficient has a significant impact on robustness of the system for strong coupling strength, but for weak coupling strength it has little influence, especially for attacking both networks. The study implies that we can obtain a more robust network by reducing clustering coefficient and increasing average degree for strong coupling strength. However, for weak coupling strength, a more robust network is obtained only by increasing average degree for the same support average degree. Additionally, we find that for attacking both networks the system becomes more vulnerable and difficult to defend compared to attacking only one network.

1. Introduction

The study of complex networks is a young and active area of scientific research and appears in almost every aspect of science and technology [1–17]. Robustness of networks is a very important topic in many contexts: in communication

* Corresponding author at: Nonlinear Scientific Research Center, Faculty of Science, Jiangsu University, Zhenjiang, 212013, China. Tel.: +86 16178030318.
E-mail address: dfocus.gao@gmail.com (G. Dong).

0378-4371/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.physa.2013.09.055

networks, where equipment failures may disrupt the network and prevent users from communicating; in distribution networks, breakdowns can prevent service to customers and so on [18–22]. The robustness of network structure mainly concerns failure nodes being removed to induce a topological change, the measure of network function is given by the size of the giant component (the largest connected subnetwork) and calculating the value of critical threshold analyzed by percolation theory [23–27]. In 2009, M.E.J. Newman proposed a random-graph model of a clustered network that is exactly solvable for many of its properties including component sizes, existence and size of a giant component, and percolation properties [28]. The model forms the basis for future investigations, including epidemic processes, network resilience, and dynamical systems on networks [29–33]. Then, J.C. Miller introduced a class of random clustered networks with the same preferential mixing. He found that percolation in the clustered networks reduces the component sizes and increases the epidemic threshold compared to the unclustered networks [29]. By comparing the threshold in an unclustered network with the same degree distribution and correlation structure, J.P. Gleeson et al. found that clustering increases the epidemic threshold or decreases resilience of the network to random edge deletion [33]. Previous works have been focused on single, isolated networks where no interaction with other networks is considered, i.e., the behavior of the system is independent of any other, coupled with it. Such conditions rarely occur in nature or in technology. Typically, systems are interdependent and events taking place in one are likely to affect the others [34–41]. For instance, email and e-commerce networks rely on the Internet which in turn relies on the electric grid. In biological systems, activated genes give rise to proteins some of which go back to the genetic level and activate or inhibit other genes [42–47]. Because infrastructures in our modern society are becoming increasingly interdependent, understanding how systemic robustness due to partial interdependency is affected is one of the major challenges for designing resilient infrastructures. Recently, Buldyrev et al. developed a framework, based on percolation theory, to study the robustness of interdependent networks [34]. The studies in coupled networks highlighted the vulnerability of tightly coupled infrastructures and showed the need to consider mutually dependent network properties in designing resilient systems. Parshani et al. studied a system composed from two partially interdependent networks [35]. For two interdependent Erdos–Renyi (ER) networks, their results showed that there exists a critical threshold, below which the system shows a second-order percolation transition, while above the threshold a first-order discontinuous percolation transition occurs. Zhou et al. studied percolation behavior of two interdependent scale-free (SF) networks under random failure of a $1-p$ fraction of nodes [45]. They found that coupling strength between the two networks q reduces from 1 to 0, there exist two critical coupling strengths q_1 and q_2, which separate three different regions with different behavior of the giant component as a function of p by introducing a new analytical method. Huang et al. developed an analytical method for studying how clustering within the networks of a system of interdependent networks affects the system's robustness. They found that clustering significantly increases the vulnerability of the system [48]. Shao et al. introduced the model in coupled network systems with fully multiple support–dependence relations, which can help to further understand real-life coupled network systems, where complex dependence–support relations exists [49]. For n clustered networks, Shao et al. generalized the study of clustering of a fully coupled pair of networks and studied the robustness of a partially interdependent network of networks with clustering. Their findings highlight that interdependent networks become more vulnerable by increasing clustering coefficient for two types of model of clustered networks, which are proposed by Newman and Hackett et al. respectively [50].

Since the robustness of clustered networks with partial support–dependence relations is much more complex and practical, the analysis of percolation behaviors remains challenging and meaning. Taking this into account, this paper is organized as follows: we study the cascading failures of clustered networks with partial support–dependence relations in Section 2. In Section 3, when a clustered network with partial support–dependence relations is subjected to two different ways of attack, we analyze percolation behaviors of the system. In Section 4, our conclusions and summary are given.

2. Cascading failures of clustered networks with partial support–dependence relations

The partial support–dependence relations between two networks A and B of sizes N_A and N_B are presented by unidirectional support links, which connecting the support nodes in one network and the dependent nodes in the other network. For a node of dependent nodes $(q_{AB}N_B)$ (or $(q_{BA}N_A)$) in network B (or A), we randomly choose $\widetilde{k}_A$ (or $\widetilde{k}_B$) nodes in network A (or B) to support it, where $\widetilde{k}_A$ (or $\widetilde{k}_B$) satisfies support degree distribution $\widetilde{P}^A(\widetilde{k}_A)$ (or $\widetilde{P}^B(\widetilde{k}_B)$). We assume a functional node of dependent nodes within one network should satisfy both of the following conditions: (i) must have at least one functional support node in other networks and (ii) must belong to the giant component of functional nodes in the network it belongs to [49]. When studying cascading failure dynamics between two networks, we assume that all their support nodes in network B which are found to be functional at the previous $(t-1)$ step are still functional for nodes in network A at step t, while all their support nodes in network A which are found to be functional at the current t stage are still functional for treating nodes in network B at stage t [49]. Then, when initially a $1-p_A$ and $1-p_B$ fraction of nodes are randomly removed from both networks, the probability that the node in network A at stage t has no functional support nodes in network B is

$$\beta_t^{BA} = q_{BA} \sum_{\widetilde{k}_{BA}=0}^{\infty} \widetilde{P}^{BA}(\widetilde{k}_{BA})(1-p_{t-1}^{(B)})^{\widetilde{k}_{BA}} = q_{BA}\widetilde{G}^{BA}(1-p_{t-1}^{(B)}), \tag{1}$$

where $\widetilde{G}^{BA}$ is the generating function of the support degree distribution $\widetilde{P}^{A}(\widetilde{k}_A)$ and $p_{t-1}^{(B)}$ is a fraction of functional nodes in network B at stage $t-1$. The probability that the node in network B at stage t has no functional support nodes in network A is

$$\beta_t^{AB} = q_{AB} \sum_{\widetilde{k}_{AB}=0}^{\infty} \widetilde{P}^{AB}(\widetilde{k}_{AB})(1-p_{t-1}^{(A)})^{\widetilde{k}_{AB}} = q_{AB}\widetilde{G}^{AB}(1-p_{t-1}^{(A)}). \tag{2}$$

Furthermore, according to condition (i), the fractions of nodes in network A which remain functional at step t is

$$x_t^{(A)} = p_A(1-\beta_t^{BA}). \tag{3}$$

Similarly, the fraction of functional nodes in network B at step t due to condition (i) is

$$x_t^{(B)} = p_B(1-\beta_t^{AB}). \tag{4}$$

The clustered network in this paper is defined by joint degree distribution, $P_k = \sum_{s,t=0}^{\infty} P_{st}\delta_{k,s+2t}$, where $\delta_{i,j}$ is the Kronecker delta and s, t design the numbers of single edges and triangles for every node. Then, $k = s+2t$ is the node's degree for a clustered network [48,50]. Accordingly, the generating function for the joint degree distribution is

$$G_0(x,y) = \sum_{s,t=0}^{\infty} P_{st} x^s y^t. \tag{5}$$

By the definition of clustering coefficient [28,50], we get the clustering coefficient

$$c = \frac{3N_\triangle}{N_3} = \frac{N\sum_{st} tP_{st}}{N\sum_{k}\binom{k}{2}P_k}. \tag{6}$$

After a fraction of $(1-p)$ nodes is randomly removed from one clustered network, the corresponding generating function becomes according to Ref. [48]

$$G_0(x,y,p) = G_0(xp+1-p, yp^2+2xp(1-p)+(1-p)^2). \tag{7}$$

And, we also get

$$g(p) = 1 - G_0(u, v^2, p) \tag{8}$$

where $u = G_q(u, v^2, p)$, $v = G_r(u, v^2, p)$ and $G_q(x,y,p) = \frac{1}{\langle s\rangle}\frac{\partial G_0(x,y,p)}{\partial x}$, $G_r(x,y,p) = \frac{1}{\langle t\rangle}\frac{\partial G_0(x,y,p)}{\partial y}$. $\langle s\rangle$ and $\langle t\rangle$ are defined as the average number of single links and triangles for each node [48]. We consider a network that has the joint Poisson degree distribution [28,48,50]

$$P_{st} = e^{-\mu}\frac{\mu^s}{s!}e^{-\nu}\frac{\nu^t}{t!} \tag{9}$$

where μ and ν are the average numbers of single edges and triangles per node. For construction of a clustered network, we adopt Newman's model [28,48,50]. When average degree $\langle k\rangle$, c, and the number of nodes N are fixed, we get numbers of nodes with single links and triangles N_s and N_t from Eq. (9). We firstly randomly choose two nodes, which are not connected and have no common connected node, to connect until the number of nodes with single links within the network is equal to N_s. Secondly, we randomly choose three nodes, which are not connected with each other, to connect with each other until the number of nodes with triangles within the network is equal to N_t. From Eq. (6), we get the clustering coefficient

$$c = \frac{2\nu}{2\nu+(\mu+2\nu)^2}. \tag{10}$$

Then, according to Eqs. (7) and (8), we obtain [48]

$$G_0(x,y) = e^{\mu(x-1)}e^{\nu(y-1)}, \tag{11}$$

$$G_0(x,y,p) = G_q(x,y,p) = G_r(x,y,p)e^{[\mu p+2p(1-p)\nu](x-1)}e^{\nu p^2(y-1)}, \tag{12}$$

$$g(p) = 1 - e^{-[\mu p+2p(1-p)\nu]g(p)}e^{\nu p^2[g(p)^2-2g(p)]}. \tag{13}$$

Then, according to condition (ii), the fraction of the giant component of network A and B at step t can be obtained

$$\begin{cases} p_t^{(A)} = x_t^{(A)} g(x_t^{(A)}), \\ p_t^{(B)} = x_t^{(B)} g(x_t^{(B)}). \end{cases} \tag{14}$$

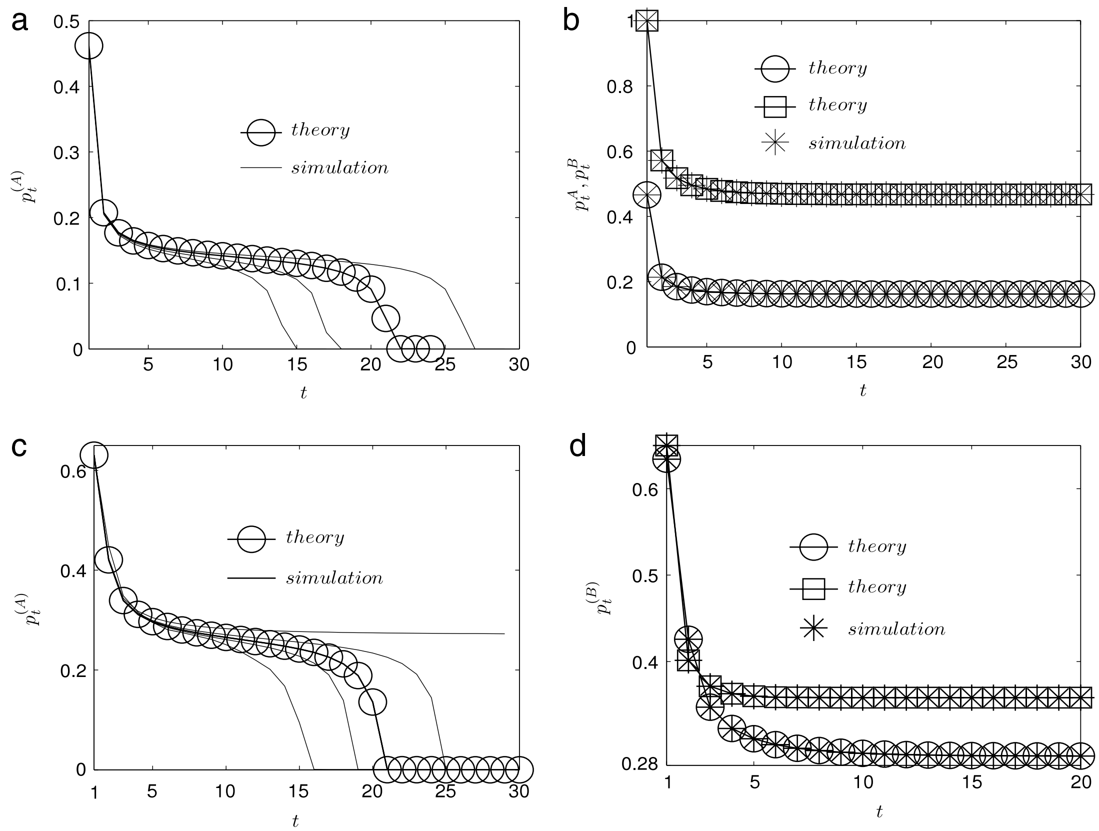

Fig. 1. (a–b) When $1 - p_A$ fraction of nodes are removed from network A, comparison between theory and simulation of $p_t^{(A)}$ and $p_t^{(B)}$ with $N_A = N_B = 10^6$, $p_B = 1$, $q_{BA} = q_{AB} = 0.8$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = 5$, $\langle k \rangle = 3$ and $c = 0.1$. (a) and (b) demonstrate the fraction $p_t^{(A)}$ and $p_t^{(B)}$ of the giant component of both networks at different steps of the cascade of failures for $p_A = 0.4618$ (below critical threshold $p_{Ac} = 0.465$ (Fig. 1(a)) and $p_A = 0.466 > p_{Ac}$ (Fig. 1(b), $p_t^{(A)}$ (◯), $p_t^{(B)}$ (□)) respectively). (c–d) When $1 - p$ fraction of nodes are removed from both networks, comparison between theory and simulation of $p_t^{(A)}$ and $p_t^{(B)}$ with the same parameters as (a) and (b). We choose parameter for $p = 0.6305 < p_c = 0.633$ in Fig. 1(c) and $p = 0.6341$ (□) and $p = 0.635$ (◯) at Fig. 1(d).

Since support links between two networks are randomly connected, from Eqs. (1) and (2), we obtain

$$\begin{cases} \widetilde{G}^{BA}(1 - p_t^{(B)}) = e^{-\widetilde{a}p_{t-1}^{(B)}}, \\ \widetilde{G}^{AB}(1 - p_t^{(A)}) = e^{-\widetilde{b}p_t^{(A)}}. \end{cases} \tag{15}$$

$$\begin{cases} x_t^{(A)} = p_A[1 - q_{BA}\widetilde{G}^{BA}(1 - p_{t-1}^{(B)})] = p_A[1 - q_{BA}\, e^{-\widetilde{a}p_{t-1}^{(B)}}], \\ x_t^{(B)} = p_B[1 - q_{AB}\widetilde{G}^{AB}(1 - p_t^{(A)})] = p_B[1 - q_{AB}\, e^{-\widetilde{b}p_t^{(A)}}]. \end{cases} \tag{16}$$

$$\begin{cases} p_t^{(A)} = p_A[1 - q_{BA}\, e^{-\widetilde{a}p_{t-1}^{(B)}}]g(p_A[1 - q_{BA}\, e^{-\widetilde{a}p_{t-1}^{(B)}}]), \\ p_t^{(B)} = p_B[1 - q_{AB}\, e^{-\widetilde{b}p_t^{(A)}}]g(p_B[1 - q_{AB}\, e^{-\widetilde{b}p_t^{(A)}}]). \end{cases} \tag{17}$$

From Fig. 1, we compare simulation with theoretical prediction by applying Eqs. (13), (15) and (16), one can see that theory and numerical simulations are consistent.

3. Analysis of percolation behaviors

In this section, when a clustered network with partial support–dependence relations is subjected to two different ways of attack, the percolation transition behaviors are studied. As step $t \to \infty$, both clustered networks reach a stable state where no further cascading failures happen according to the above two conditions and we assume $x_t^{(i)} = x_{t+1}^{(i)} = x_\infty^{(i)}$, $p_t^{(i)} = p_{t+1}^{(i)} = p_\infty^{(i)} (i = A, B)$. Thus, as $N_A \to \infty$ and $N_B \to \infty$, from Eqs. (16) and (17), we get

$$\begin{cases} x_\infty^{(A)} = p_A[1 - q_{BA}\widetilde{G}^{BA}(1 - p_\infty^{(B)})] = p_A[1 - q_{BA}\, e^{-\widetilde{a}p_\infty^{(B)}}], \\ x_\infty^{(B)} = p_B[1 - q_{AB}\widetilde{G}^{AB}(1 - p_\infty^{(A)})] = p_B[1 - q_{AB}\, e^{-\widetilde{b}p_\infty^{(A)}}]. \end{cases} \tag{18}$$

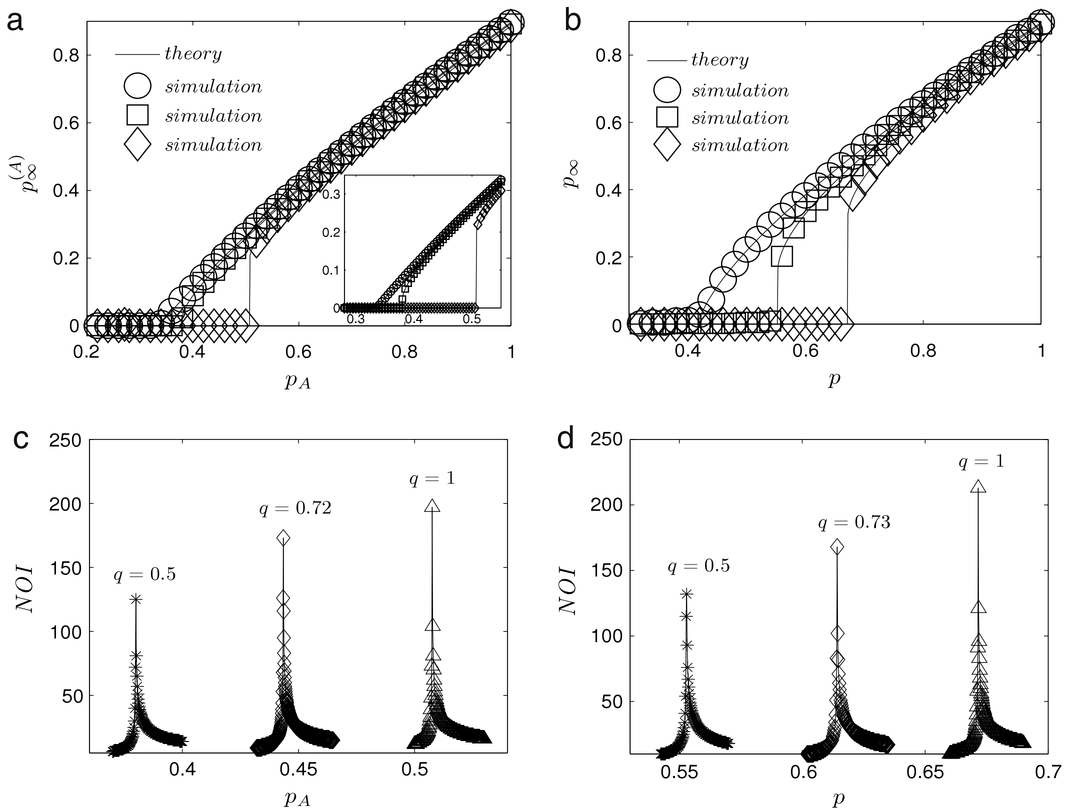

Fig. 2. (a–b) For two different ways of attack, comparisons between simulations and theory of the fraction of giant component as a function of attacking strength for different coupling strength $q_{BA} = q_{AB} = q$ from Eqs. (19) and (20) are shown. (a) $p_\infty^{(A)}$ as a function of p_A with parameters $p_B = 1$, $\langle k\rangle = 3$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = 5$, $c = 0.1$ and different $q = 1$ (◇), $q = 0.5$ (□) and $q = 0.2$ (◯). (b) p_∞ as a function of p with parameters $p_A = p_B = p$, $\langle k\rangle = 3$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = 5$, $c = 0.1$ and different $q = 1$ (◇), $q = 0.5$ (□) and $q = 0.2$ (◯). In simulation, $N_A = N_B = 10^6$ and the results are averaged over 50 realizations. (c–d) For two different kinds of attacks, *NOI* as a function of attacking strength for different coupling strength $q_{BA} = q_{AB} = q$ is shown. The parameters of (c) and (d) are the same as (a) and (b).

$$\begin{cases} p_\infty^{(A)} = p_A[1 - q_{BA}\, e^{-\widetilde{a}p_\infty^{(B)}}]g(x_\infty^{(A)}) = p_A[1 - q_{BA}\, e^{-\widetilde{a}p_\infty^{(B)}}]g(p_A[1 - q_{BA}\, e^{-\widetilde{a}p_\infty^{(B)}}]), \\ p_\infty^{(B)} = p_B[1 - q_{AB}\, e^{-\widetilde{b}p_\infty^{(A)}}]g(x_\infty^{(B)}) = p_B[1 - q_{AB}\, e^{-\widetilde{b}p_\infty^{(A)}}]g(p_B[1 - q_{AB}\, e^{-\widetilde{b}p_\infty^{(A)}}]). \end{cases} \tag{19}$$

From Eq. (19), we assume that two networks have the same $\langle k\rangle$, $\widetilde{k}$ and c, then $p_\infty^{(A)} = p_\infty^{(B)} = p_\infty$

$$p_\infty = p[1 - qe^{-\widetilde{k}p_\infty}]g(x_\infty) = p[1 - qe^{-\widetilde{k}p_\infty}]g(p[1 - qe^{-\widetilde{k}p_\infty}]). \tag{20}$$

For Eq. (19), the graphical solution of Eqs. (19) and (20) is shown in Fig. 3. From Fig. 3, we observe that the critical value of the parameters can be obtained by finding the tangent point of the two curves $p_\infty^{(A)}(p_\infty^{(B)})$ and $p_\infty^{(B)}(p_\infty^{(A)})$ as follows

$$\frac{\mathrm{d}p_\infty^{(A)}}{\mathrm{d}p_\infty^{(B)}}\frac{\mathrm{d}p_\infty^{(B)}}{\mathrm{d}p_\infty^{(A)}} = 1. \tag{21}$$

The graphical solution of Eqs. (19) and (20) can be easily solved and presented in Fig. 2(a) and (b). When clustered network A is initially under random attack, $p_\infty^{(A)}$ as a function of p_A for the different coupling strength is shown in Fig. 2(a). When $1 - p$ fraction of nodes are initially removed from both clustered networks, p_∞ as a function of p for the different coupling strength is shown in Fig. 2(b). For Fig. 2(a)–(b), we test the theoretical prediction with numerical simulations. The theory agrees very well with the simulation results. By comparing Fig. 2(a)–(b), we see that the critical threshold p_{Ac} (Fig. 2(a)) is smaller than p_c (Fig. 2(b)) for the different coupling strength. The number of iterative failures (*NOI*) as a function of p_A and p is shown in Fig. 2(c) and (d) respectively. From Fig. 2(c) and (d), we observe that the transition point, where the size of the giant component jumps, can be easily identified by the sharp peak characterizing the transition point. Thus, It is a useful method for identifying the transition point by graphically presenting *NOI* as a function of attacking strength.

The robustness of a network is usually characterized by the value of the critical threshold, which is analyzed by percolation theory. Without loss of generality, when network A is under random attack, from Eqs. (13) and (17), $p_\infty^{(A)}$ as

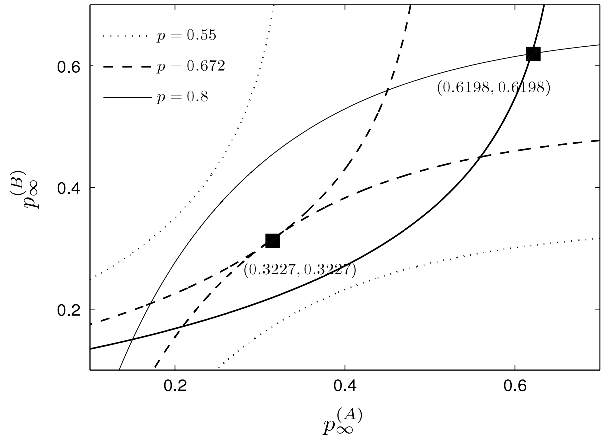

Fig. 3. Demonstration of the functional relation between $p_\infty^{(A)}$ and $p_\infty^{(B)}$ in Eq. (19) with $q_{BA} = q_{AB} = q = 1$, $\langle k \rangle = 3$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = 5$, $c = 0.1$ and different $p_{BA} = p_{AB} = p$.

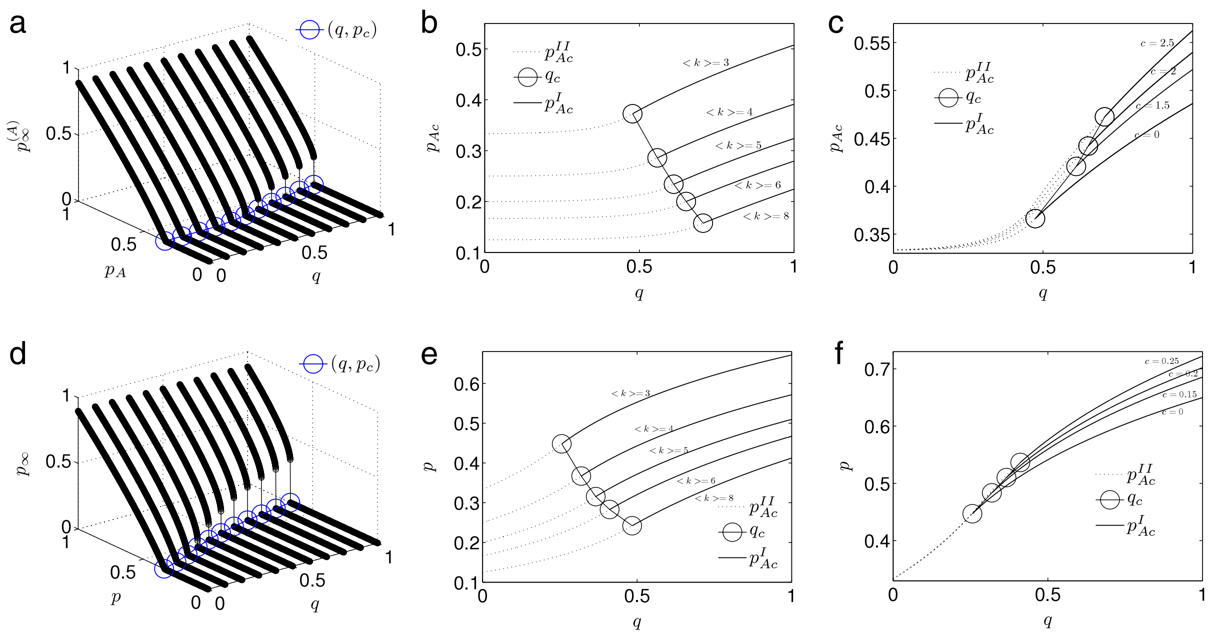

Fig. 4. The percolation behaviors are analyzed with different $\langle k \rangle$ and c for two different ways of attack, only network A (shown on Fig. 4(a–c)) and both networks (shown on Fig. 4(d–f)) are initially under random attack. (a) The size of the giant component, $p_\infty^{(A)}$, as a function of attacking strength, p_A, for different values of $q_{AB} = q_{BA} = q$ with parameters $p_B = 1$, $\langle k \rangle = 3$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = 5$, $c = 0.1$. (b) p_{Ac} as a function of q with the same parameters as Fig. 4(a) but different $\langle k \rangle$. (c) p_{Ac} as a function of q with the same parameters as Fig. 4(b) but different c. (d) The size of the giant component, p_∞, as a function of attacking strength, $p_A = p_B = p$, for different values of $q_{AB} = q_{BA} = q$ with parameters $\langle k \rangle = 3$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = 5$, $c = 0.1$. (e) p_c as a function of q with the same parameters as Fig. 4(d) but different $\langle k \rangle$. (f) p_c as a function of q with the same parameters as Fig. 4(e) but different c.

a function of attacking strength and coupling strength are graphically presented in Fig. 4(a). From Fig. 4(a), we observe that the network undergoes a first order transition for strong coupling $q > q_c$, q_c is critical coupling strength, at which $p_\infty^{(A)}$, where the fraction of nodes in the giant component of network A, abruptly changes from a finite value to zero. While for weak coupling $q > q_c$, the system undergoes a second order transition, where $p_\infty^{(A)}$ continuously approaches zero. From Fig. 4(b), one can see that the critical fraction p_{Ac}, including the first order phase transition line p_{Ac}^{I} and second order phase transition line p_{Ac}^{II}, increases as coupling strength q increases. This means that the system becomes more vulnerable as q increases with the same $\langle k \rangle$. Moreover, we also notice that p_{Ac} decreases as $\langle k \rangle$ increases for the same q, which means that the system becomes robust by increasing the average degree of the clustered network for the same clustered coefficient. Furthermore, p_{Ac} as a function of q is graphically described in Fig. 4(c) with the different c. We can see that the p_{Ac} increases, and the system becomes more vulnerable as q increases for the same c. And, Fig. 4(c) also demonstrates that the value of p_{Ac}

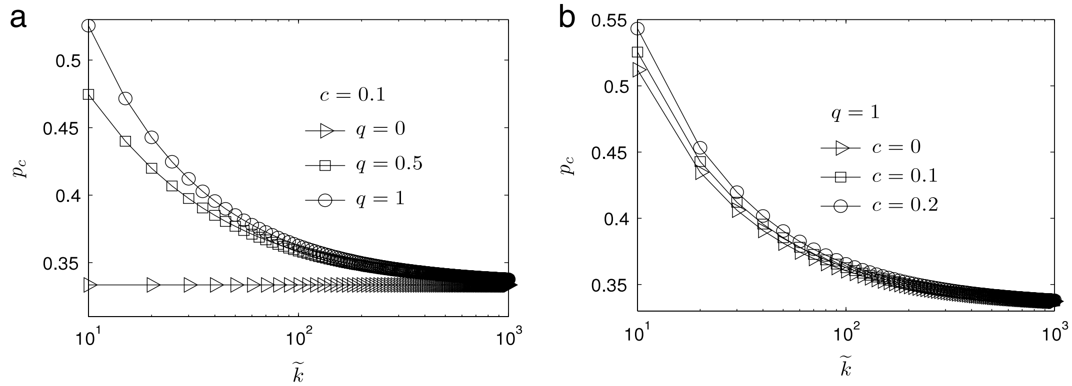

Fig. 5. The critical threshold p_c as a function of $\widetilde{k}_{BA} = \widetilde{k}_{AB} = \widetilde{k}_{BA} = \widetilde{k}$ for the different q (Fig. 5(a)) and c (Fig. 5(b)) with parameters $p_A = p_B = p$ and the same $\langle k \rangle = 3$.

becomes smaller, and the system becomes more robust as clustering coefficient decreases for the same coupling strength. Similarly, when both networks are under random attack, p_∞ as a function of q and p is graphically presented (Fig. 4(d) from Eqs. (13) and (17)). From Fig. 4(d), we also notice that the system undergoes a change from second order to first order phase transition when coupling strength q increases. And, we can see that the critical fraction p_c decreases, and the system becomes more robust as $\langle k \rangle$ increases for the same c and q from Fig. 4(e). Additionally, the system becomes more vulnerable as q increases for the same c and $\langle k \rangle$ as shown in Fig. 4(f). When the system is subject to two different ways of attack, by comparing Fig. 4(b) with Fig. 4(e), we find that $p_{Ac} > p_c$ for the same $\langle k \rangle$, which suggests that the system becomes more vulnerable and difficult to defend for attacking both clustered networks compared to attacking only one clustered network. And, for the two different ways of attack, by comparing Fig. 4(c) and (f), we find that the difference in critical fraction, p_{Ac} or p_c, between different c increases as q increases. This implies that clustering has a significant impact on robustness for strong coupling strength. However, for weak coupling strength, clustering coefficient has little influence on robustness of the clustered network. Thus, when random clustered networks with partial support–dependence relations, for strong coupling strength, we can obtain a more robust clustered network by reducing clustering coefficient and increasing average degree. But for weak coupling strength, we can obtain more robust network only by increasing average degree for the same support average degree.

Moreover, the critical threshold as a function of $\widetilde{k}$ for the different q and c are shown in Fig. 5. From Fig. 5(a), as support average degree increases and approaches infinity for different q, p_c gradually decreases and finally coincides with values at $q = 0$. This means that the giant component of the clustered network does not depend on the other network and behaves similarly to the single clustered network, which is similar to $q = 0$. And, we give p_c as a function of c in Fig. 5(b). Similarly, when $\widetilde{k} \to \infty$, p_c is the same as the critical threshold's value of site percolation of single clustered networks.

From the above analysis, for two different ways of attack, there exist critical coupling strengths q_c, which separate two different regions with different behaviors of the giant component as a function of attacking strength. When only one network is under random attack, Fig. 6(a) and (b) demonstrate the regions of two different behaviors change as $\langle k \rangle$ and c change. When both networks are under random attack, Fig. 6(c) and (d) show that two different regions change as $\langle k \rangle$ or c changes. From Fig. 6, we notice that the region of first order transition becomes smaller, while the region of second order transition becomes larger as $\langle k \rangle$ or c increases. By comparing Fig. 6(a) with Fig. 6(c), for the same range of average degree, one can see that the first-order region for attacking only one network is bigger than that for attacking both networks; however, the second-order region for attacking only one network is smaller than that for attacking both networks. Meanwhile, by comparing Fig. 6(b) with Fig. 6(d), for the same range of clustering coefficient, we find that the first-order region for attacking only one network is smaller than that for attacking both networks; however, the second-order region for attacking only one network is bigger than that for attacking both networks.

4. Conclusions

In this paper, we study percolation behaviors of random clustered networks with partial support–dependence relations. We choose two kinds of different attacking strategies, only one clustered network ($p_B = 1$) and both clustered networks ($p_A = p_B = p$) are under random attack. For the above two attacking strategies, we find that the system shows behaviors of first order and second order phase transition. And, we observe that the region of first order phase transition becomes smaller, while the region of second order phase transition becomes larger as $\langle k \rangle$ or c increases. As average supported degree $\widetilde{k} \to \infty$, coupled clustered networks become independent and behave similarly to a single clustered network. And, the system becomes robust as $\langle k \rangle$ increases for the different clustered coefficients. For strong coupling strength, p_{Ac} or p_c increases and the system becomes vulnerable as c increases. However, as c changes, p_{Ac} or p_c has not changed significantly for weak coupling strength, which means that clustering has no discernible impact on robustness of the system for weak

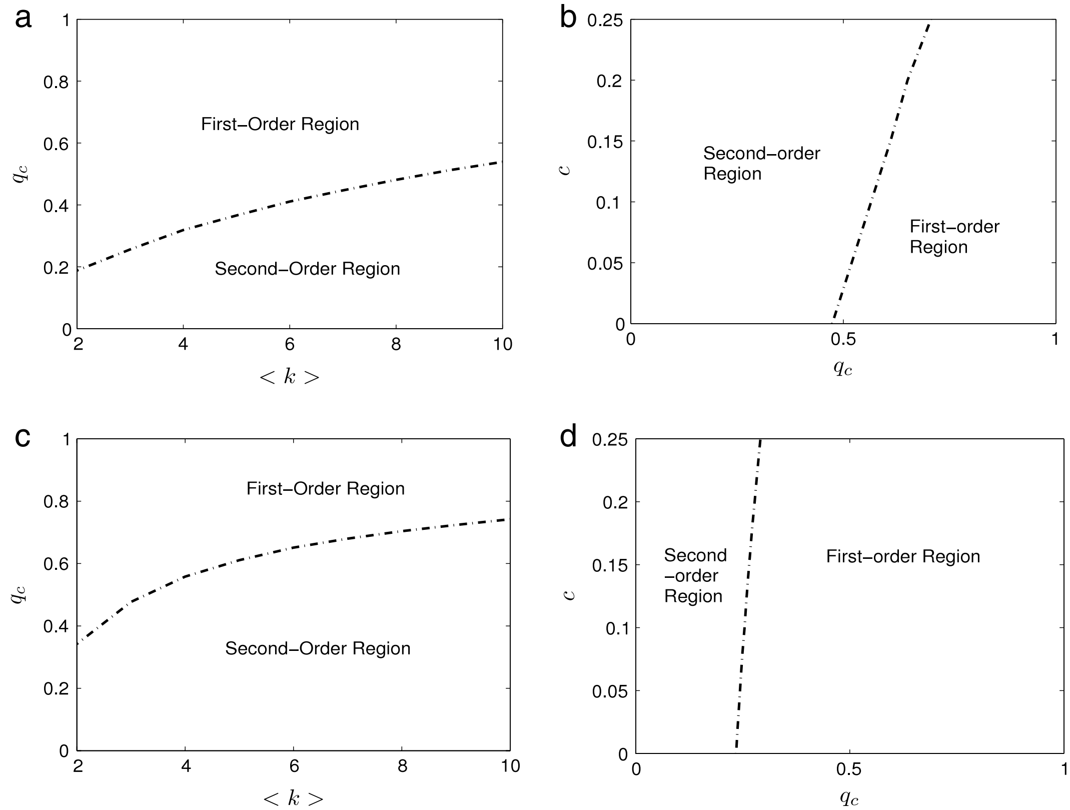

Fig. 6. For two different ways of attack, the phase diagram shows the first-order and second-order phase transition regions and boundary. (a) q_c as a function of $\langle k \rangle$ with parameters $p_B = 1$, $q_{AB} = q_{BA} = q$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = \widetilde{k}_{BA} = 5$, $c = 0.1$. (b) c as a function of q_c with parameters $p_B = 1$, $q_{AB} = q_{BA} = q$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = \widetilde{k}_{BA} = 5$, $\langle k \rangle = 3$. (c) q_c as a function of $\langle k \rangle$ with parameters $p_A = p_B = p$, $q_{AB} = q_{BA} = q$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = \widetilde{k}_{BA} = 5$, $c = 0.1$. (d) c as a function of q_c with parameters $p_A = p_B = p$, $q_{AB} = q_{BA} = q$, $\widetilde{k}_{BA} = \widetilde{k}_{AB} = \widetilde{k}_{BA} = 5$, $\langle k \rangle = 3$.

coupling strength. Additionally, the results imply that for attacking both networks the system becomes more vulnerable and difficult to defend, in contrast with attacking one of two clustered networks.

Acknowledgments

L.T. thanks the National Natural Science Foundation of China (Grant Nos. 11171135, 71073071, 71073072, 51276081) and the Major Program of the National Social Science Foundation of China (Grant No. 12&ZD062) for support. M.F. thanks the National Youth Natural Science Foundation of China (Grant No. 71303095) for support, G.D. thanks China Scholarship Funding (Grant No. 2011832326) and the Natural Science Foundation of Jiangsu Province (Grant Nos. BK20130535, SBK201342872) and National Natural Science Foundation of China (Grant No. 51305168). HES thanks ONR (Grant Nos. N00014-09-1-0380, N00014-12-1-0548), DTRA (Grant Nos. HDTRA-1-10-1-0014, HDTRA-1-09- 1-0035) and NSF (Grant No. CMMI 1125290) for support.

References

[1] D.J. Watts, S.H. Strogatz, Collective dynamics of small-world networks, Nature 393 (1998) 440.
[2] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (1999) 509.
[3] L.A.N. Amaral, A. Scala, M. Barthelemy, H.E. Stanley, Classes of small-world networks, Proc. Natl. Acad. Sci. USA 97 (2000) 11149–11152.
[4] D. Markovic, S. Milosevic, H.E. Stanley, Self-avoiding walks on random networks of resistors and diodes, Physica A 144 (1987) 1–16.
[5] M.E.J. Newman, D.J. Watts, Renormalization group analysis of the small-world network model, Phys. Lett. A 263 (1999) 341–346.
[6] A.-L. Barabási, E. Ravasz, T. Vicsek, Deterministic scale-free networks, Physica A 299 (2001) 559–564.
[7] R. Albert, A.-L. Barabási, Statistical mechanics of complex networks, Rev. Modern Phys. 74 (1) (2002) 47–97.
[8] Y. Chen, G. Paul, R. Cohen, S. Havlin, S.P. Borgatti, F. Liljeros, H.E. Stanley, Percolation theory applied to measures of fragmentation in social networks, Phys. Rev. E 75 (2007) 046107.
[9] D. Li, K. Kosmidis, A. Bunde, S. Havlin, Dimension of spatially embedded networks, Nat. Phys. 7 (2011) 481.
[10] M.E.J. Newman, The structure and function of complex networks, SIAM Rev. 45 (2) (2003) 167–256.
[11] D.J. Watts, Small World:The dynamics of Networks between Order and Randomness, Princeton University Press, 1999.
[12] T. Konno, An imperfect competition on scale-free networks, Physica A (2013). http://dx.doi.org/10.1016/j.physa.2013.06.017.
[13] Z. Lu, Y. Su, S. Guo, Deterministic scale-free small-world networks of arbitrary order, Physica A 392 (2013) 3555–3562.

[14] S. Havlin, L.A. Braunstein, S.V. Buldyrev, R. Cohen, T. Kalisky, S. Sreenivasan, H.E. Stanley, Optimal path in random networks with disorder: a mini review [Proc. Kolkata Conf on Networks], Physica A 346 (2004) 82–92.
[15] G. Paul, S. Sreenivasan, S. Havlin, H.E. Stanley, Optimization of network robustness to random breakdowns, Physica A 370 (2006) 854–862.
[16] S. Carmi, Z. Wu, S. Havlin, H.E. Stanley, Transport in networks with multiple sources and sinks, Europhys. Lett. 84 (2008) 28005.
[17] J. Shao, S.V. Buldyrev, R. Cohen, M. Kitsak, S. Havlin, H.E. Stanley, Fractal boundaries of complex networks, Europhys. Lett. 84 (2008) 48004.
[18] G. Paul, T. Tanizawa, S. Havlin, H.E. Stanley, Optimization of robustness of complex networks, Eur. Phys. J. B 38 (2004) 187–191.
[19] R. Albert, H. Jeong, A.-L. Barabási, Error and attack tolerance of complex networks, Nature 406 (2000) 378.
[20] X. Huang, I. Vodenska, S. Havlin, H.E. Stanley, Cascading failures in bi-partite graphs: model for systemic risk propagation, Nature Scientific Reports 3 (2013) 1219.
[21] A. Beygelzimer, G. Grinstein, R. Linsker, I. Rish, Improving network robustness by edge modification, Physica A 357 (2005) 593–612.
[22] M. Kitsak, L.K. Gallos, S. Havlin, F. Liljeros, L. Muchnik, H.E. Stanley, H.A. Makse, Identification of influential spreaders in complex networks, Nat. Phys. 6 (2010) 888–893.
[23] N. Barkai, S. Leibler, Robustness in simple biochemical networks, Nature 387 (1997) 913–917.
[24] C.M. Song, S. Havlin, H.A. Makse, Origins of fractality in the growth of complex networks, Nat. Phys. 2 (2006) 275–281.
[25] H. Zhao, Z.Y. Gao, Organizations of rich nodes in complex networks, Physica A 381 (2007) 473–481.
[26] B. Podobnik, D. Horvatic, M. Dickison, H.E. Stanley, Preferential attachment in the interaction between dynamically generated interdependent networks, Europhys. Lett. 100 (2012) 50004.
[27] B. Wang, H. Tang, C. Guo, Z. Xiu, Entropy optimization of scale-free networks robustness to random failures, Physica A 363 (2006) 591–596.
[28] M.E.J. Newman, Random graphs with clustering, Phys. Rev. Lett. 103 (2009) 058701.
[29] J.C. Miller, Percolation and epidemics in random clustered networks, Phys. Rev. E 80 (2009) 020901(R).
[30] G. Paul, S. Sreenivasan, H.E. Stanley, Resilience of complex networks to random breakdown, Phys. Rev. E 72 (2005) 056130.
[31] B. Karrer, M.E.J. Newman, Random graphs containing arbitrary distributions of subgraphs, Phys. Rev. E 82 (2010) 066118.
[32] M. Serrano, D. Krioukov, M. Boguna, Percolation in self-similar networks, Phys. Rev. Lett. 106 (2011) 048701.
[33] J.P. Gleeson, S. Melnik, J.A. Ward, M.A. Porter, P.J. Mucha, Accuracy of mean-field theory for dynamics on real-world networks, Phys. Rev. E 85 (2012) 026106.
[34] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[35] R. Parshani, S.V. Buldyrev, S. Havlin, Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition, Phys. Rev. Lett. 105 (2010) 048701.
[36] J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of a network of networks, Phys. Rev. Lett. 107 (2011) 195701.
[37] X. Huang, J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Robustness of interdependent networks under targeted attack, Phys. Rev. E 83 (2011) 065101(R).
[38] G. Dong, J. Gao, L. Tian, R. Du, Y. He, Percolation of partially interdependent networks under targeted attack, Phys. Rev. E 85 (2012) 016112.
[39] W. Li, A. Bashan, S.V. Buldyrev, H.E. Stanley, S. Havlin, Cascading failures in interdependent lattice networks: the critical role of the length of dependency links, Phys. Rev. Lett. 108 (2012) 228702.
[40] Y. Hu, B. Ksherim, R. Cohen, S. Havlin, Percolation in interdependent and interconnected networks: Abrupt change from second- to first-order transitions, Phys. Rev. E 84 (2011) 066116.
[41] S. Havlin, N.A.M. Araujo, S.V. Buldyrev, C.S. Dias, R. Parshani, G. Paul, H.E. Stanley, Catastrophic cascade of failures in interdependent networks. arXiv:1012.0206v1.
[42] M. Dickison, S. Havlin, H.E. Stanley, Epidemics on interconnected networks, Phys. Rev. E 85 (2012) 066109.
[43] C.D. Brummitt, R.M. DSouza, E.A. Leicht, Suppressing cascades of load in interdependent networks, Proc. Natl. Acad. Sci. USA 109 (2013) 680–689.
[44] J. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (2012) 40–48.
[45] D. Zhou, H.E. Stanley, G. D'Agostino, A. Scala, Assortativity decreases the robustness of interdependent networks, Phys. Rev. E 86 (2012) 066103.
[46] G. Dong, J. Gao, R. Du, L. Tian, H.E. Stanly, S. Havlin, Robustness of network of networks under targeted attack, Phys. Rev. E 87 (2013) 052804.
[47] D. Zhou, J. Gao, H.E. Stanley, S. Havlin, Percolation of partially interdependent scale-free networks, Phys. Rev. E 87 (2013) 052812.
[48] X. Huang, S. Shao, H. Wang, S.V. Buldyrev, H.E. Stanley, S. Havlin, The robustness of interdependent clustered networks, Europhys. Lett. 101 (2013) 18002.
[49] J. Shao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Cascade of failures in coupled network systems with multiple support–dependence relations, Phys. Rev. E 83 (2011) 036116.
[50] S. Shao, X. Huang, H.E. Stanley, S. Havlin, Robustness of partially interdependent network formed of clustered networks. arXiv:1308.0034.