Chaos BRIEF COMMUNICATION scitation.org/journal/cha

Robustness of partially interdependent networks under combined attack

Cite as: Chaos **29**, 021101 (2019); doi: 10.1063/1.5085850
Submitted: 15 December 2018 · Accepted: 13 January 2019 ·
Published Online: 5 February 2019

Yangyang Liu,[1,a)] Chengli Zhao,[1,b)] Dongyun Yi,[1] and H. Eugene Stanley[2]

AFFILIATIONS

[1]Department of Systems Science, College of Liberal Arts and Sciences, National University of Defense Technology, Changsha, Hunan 410073, China
[2]Department of Physics, Center for Polymer Studies, Boston University, Boston, Massachusetts 02215, USA

[a)]**Also at:** Department of Physics, Center for Polymer Studies, Boston University, Boston, Massachusetts 02215, USA.
[b)]**Electronic mail:** chenglizhao@nudt.edu.cn

ABSTRACT

We thoroughly study the robustness of partially interdependent networks when suffering attack combinations of random, targeted, and localized attacks. We compare analytically and numerically the robustness of partially interdependent networks with a broad range of parameters including coupling strength, attack strength, and network type. We observe the first and second order phase transition and accurately characterize the critical points for each combined attack. Generally, combined attacks show more efficient damage to interdependent networks. Besides, we find that, when robustness is measured by the critical removing ratio and the critical coupling strength, the conclusion drawn for a combined attack is not always consistent.

Many real systems such as power grid networks and their communication networks are coupled together to function, where each layer being a single network and coupled with other layers forms interdependent networks. The robustness of interdependent networks against cascading failures caused by different attacks has long been the focus of research. However, previous studies mainly focused on the robustness of networks under one single attack type. In a real scene, interdependent networks suffering multiple attacks simultaneously are more common. In this paper, we develop a framework to study the robustness of partially interdependent networks under combined attacks. Richness phase transition behaviors are observed and critical points with a broad range of parameters are characterized accurately. Our work sheds light on designing robust networks against risks and how to better protect vulnerable networks.

I. INTRODUCTION

Network robustness has always been a significant role in complex networks.[1–5] From the perspective of connectivity,[6] scholars study the vulnerability of the structure exploiting the percolation theory. By percolation, nodes are assigned into two states: occupied and unoccupied. A fraction of nodes is occupied initially, and the final size of the giant component is observed to measure the connectivity of networks. A fundamental assumption is that nodes are functional if and only if they belong to the giant component. This simple but efficient model exploiting from statistical physics has produced many profound results and provides us deep insight into designing robust networks.[7–9]

Nowadays, components of the modern system are coupled with each other.[10] This has been observed in many social, economic, Internet of things,[11] and industrial systems.[12] For instance, in the power grid, the communication control computers and power stations are coupled with one-to-one correspondence. A node in one failed network will cause its dependent node to fail, and the recursive process may lead to the abrupt fragmentation of the whole system. An initial investigation[13] was made on fully interdependent networks and developed a theoretical framework based on percolation theory. Later, releasing the restriction of a dependency relation, a more realistic model of partially interdependent networks was established.[14] Then, the generalization to the NON

system composed of coupled interdependent networks was proposed.[15]

In terms of the robustness of interdependent networks, initial attack type and dependency pattern[16–20] are the focus of research. Studies have mainly considered three attack types: random attack (RA),[21] targeted attack (TA),[22] and localized attack (LA).[23] Random attack is the direct application of percolation theory on the robustness of networks. Targeted attack was first studied on fully interdependent networks with Erdös-Rényi (ER) and scale-free (SF) random networks.[24] Then, it was studied on partially interdependent networks.[25] More recently, a new scenario of attack type, namely, localized attack, was proposed to model the effects of earthquakes, floods, or military attacks on industrial networks.[23] This kind of attack has been studied on fully interdependent networks and spatial networks.[26,27] Studies on the robustness of interdependent networks have also been successfully applied to many empirical networks such as power grids[28] and traffic networks.[29] However, previous studies on interdependent networks mainly focused on a single attack type, neglecting the fact that components of systems may suffer multiple attack types due to their individual properties. For instance, on interdependent networks formed by power stations and communication computers, the failure of the power station layer is prone to be random caused by overloading while the communication control computers layer is prone to suffer targeted attack caused by a malicious computer virus.

In this paper, we study the robustness of a pair of partially interdependent networks within each layer suffering a certain attack type. We classify attacks into two categories: single-mode and mixed-mode. For a single-mode attack, it is initiated by the same attack type for each layer, while the mixed-mode attack is the combination of random, targeted, and localized attacks. We then develop a generalized theoretical framework exploiting percolation theory to study a pair of partially interdependent networks when suffering single-mode and mixed-mode attacks. Furthermore, using the framework we obtained, the effect of both attack type and coupling strength on partially interdependent networks is comprehensively studied. Finally, we obtain critical lines and phase transition conditions for each attack mode on interdependent networks formed by ER and SF random networks.

II. MODEL

Our model is assumed in a pair of interdependent networks formed by layers A and B with degree distributions $P_A(k)$ and $P_B(k)$, respectively. An interdependent network with more than two layers is beyond our consideration. The number of nodes in each layer is N_A and N_B. The $q_A(q_B)$ fraction of nodes in layer A(B) depends on nodes of network B(A), meaning that if the node in layer B fails, the corresponding depending node in layer A also fails. For simplicity, we assume two constraint conditions: one node depends on one node of the other layers at most; if node i of layer A depends on node j of layer B and node j of layer B depends on node k of layer A, then $k = i$ (non-feedback condition). $S_A(x)[S_B(x)]$ denotes the fraction of the giant connect component when remaining x fraction of nodes is in layer A(B). It is supposed that initially $1 - p_A(1 - p_B)$ fraction of nodes in layer A(B) is removed by different attacks. First, nodes that lose connection with the giant component will lose functionality due to the removed nodes of the same layer (connectivity failure). Next, the dependency nodes of the counterpart layer fail due to dependency relations (dependency failure). Then, the connectivity and dependency failures spread on intra-layer and inter-layer cause a global cascading failure (Fig. 1).

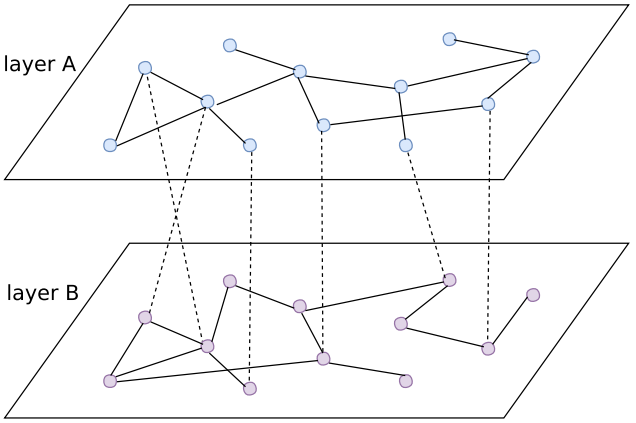

FIG. 1. Partially Interdependent Network illustration. Nodes are connected through connectivity links (solid black line) in the same layer and dependency links (dashed black line) between layers.

Mathematically, the procedure of cascade failure on interdependent networks can be described through an iterative system as follows:[13,14]

$$\begin{aligned} \Phi_t' &= p_A\{1 - q_A[1 - S_B(\Psi_{t-1}')p_B]\}, \Phi_t = \Phi_t' S_A(\Phi_t'), \\ \Psi_t' &= p_B\{1 - q_B[1 - S_A(\Phi_t')p_A]\}, \Psi_t = \Psi_t' S_B(\Psi_t'). \end{aligned} \tag{1}$$

Here, Φ_t' and Ψ_t' represent the fraction of nodes remaining in layer A and layer B at time t, respectively. The remaining functional part of layers A and B out of all original nodes at time t is Φ_t and Ψ_t.

When $t = \infty$, the system reaches its steady state. Let $x = \Phi_\infty'$, $y = \Psi_\infty'$. We have

$$\begin{aligned} x &= p_A\{1 - q_A[1 - S_B(y)p_B]\}, \\ y &= p_B\{1 - q_B[1 - S_A(x)p_A]\}. \end{aligned} \tag{2}$$

For random removing, $S_A(x) = 1 - G_{A,0}[1 - x(1 - f)]$, where $f = G_{A,1}[1 - x(1 - f)]$, $G_{A,0}(x) = \sum_k P_A(k)x^k$, $G_{A,1}(x) = G_{A,0}'(x)/G_{A,0}'(1)$.

In simulation, the iteration number varies with the initial attack fraction and reaches its summit at the critical point. This can be numerical evidence to identify the critical point of the first order transition, and the peak of the second giant component can be used to characterize the critical point of the second order transition.[30]

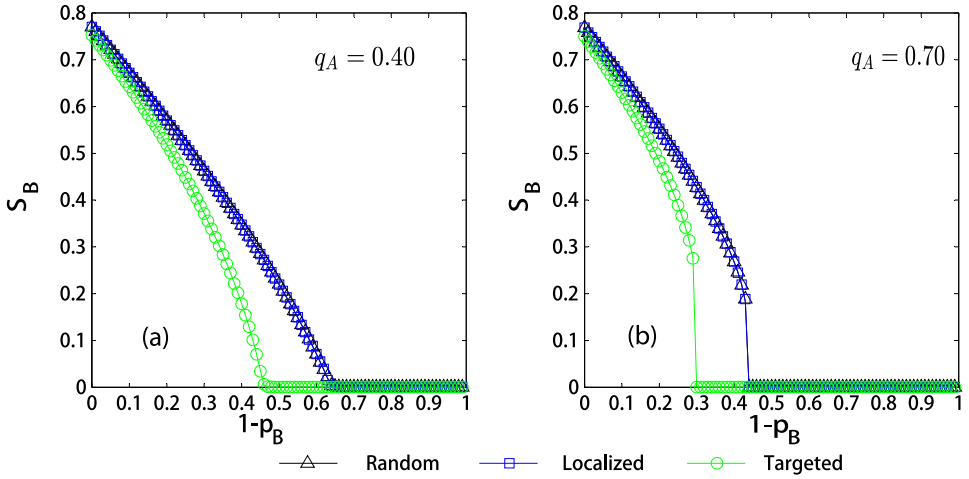

FIG. 2. The giant components of layer B as a function of initial attack size $1 - p_B$ for three single-mode attacks. Results are obtained with $N_A = N_B = 100\,000$, $< k_A >=< k_B >= 4$, $p_A = 0.8$, $q_B = 0.8$. Lines and symbols are results of theory and simulation, respectively. They agree well with each other.

In this paper, attacks are divided into two categories depending on the way the nodes are removed from each layer.

A. Single-mode attack

Random attack (RA). The randomized attack on networks is assumed that $1 - p_A$ and $1 - p_B$ fractions of nodes are removed uniformly at random.

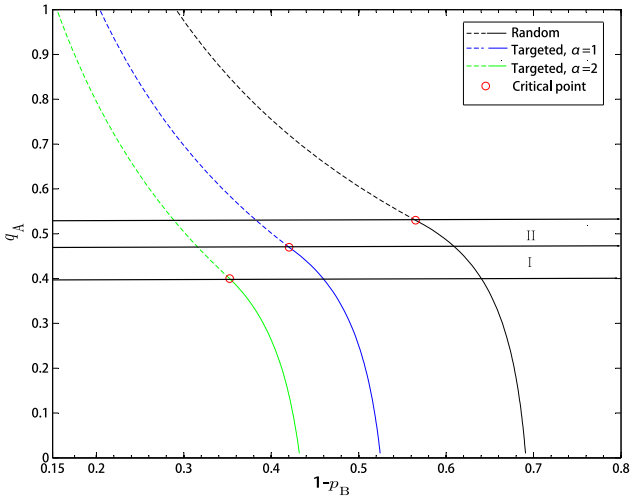

FIG. 3. The critical lines on the parameter space $(1 - p_B, q_A)$ for three single-mode attacks on ER-ER networks. From left to right, they are targeted attack with $\alpha = 2$, targeted attack with $\alpha = 1$, and random attack (localized attack), respectively. Circles characterize the junction of first and second order phase transition. The dashed part above the circle suggests that the system undergoes a first order transition when crosses over the line. The solid part under the red circle indicates the system undergoes a second order transition. We fix $p_A = 0.8, q_B = 0.8, \lambda_A = \lambda_B = 4$.

Targeted attack (TA). The targeted attack is regarded to remove $1 - p_A$ and $1 - p_B$ fractions of nodes according to their degree. A value $W_\alpha(k_i)$ is assigned to each node, which means the probability that a node i with k_i links is initially attacked as follows:[22]

$$W_\alpha(q_i) = \frac{q_i^\alpha}{\sum_{i=1}^{N} q_i^\alpha}, \quad -\infty < \alpha < +\infty, \tag{3}$$

when $\alpha > 0$, nodes with higher degree are prone to be removed.

Localized attack (LA). The localized attack is started with a randomly chosen seed node in layers A and B. Then, the seed and its nearest neighbors, next nearest neighbors, next-next-nearest neighbors, and so on are removed until $1 - p_A$ and $1 - p_B$ fractions of nodes have been removed from the network.

B. Mixed-mode attack

Random attack and localized attack (RALA). $1 - p_A$ fraction of nodes in network A is removed randomly, and $1 - p_B$ fraction of nodes in network B is removed by localized attack.

Random attack and targeted attack (RATA). $1 - p_A$ fraction of nodes in network A is removed randomly, and $1 - p_B$ fraction of nodes in network B is removed by targeted attack.

Localized attack and targeted attack (LATA). $1 - p_A$ fraction of nodes on network A is removed by localized attack, while $1 - p_B$ fraction of nodes on network B is removed by targeted attack.

III. ER-ER PARTIALLY INTERDEPENDENT NETWORKS

In this section, we consider the interdependent networks formed by two ER networks with Poisson degree distribution $P(k) = \frac{\lambda^k e^{-\lambda}}{k!}$, where $\lambda_A = \lambda_B = \lambda$ are average degrees. Simply

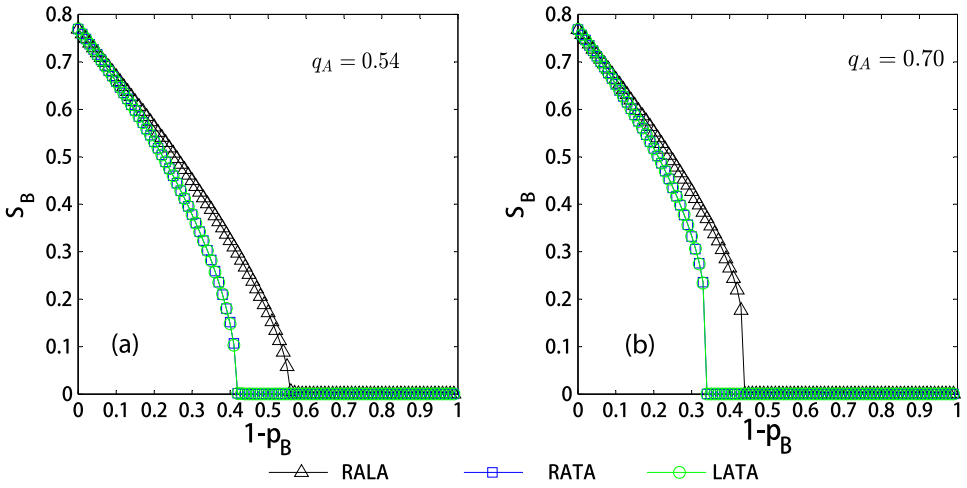

FIG. 4. The giant components of layer B under three mixed-mode attacks over weak and strong coupling strength on ER-ER networks. Symbols are results of simulation with $N_A = N_B = 100\,000$, $q_B = 0.8$, $p_A = 0.8$, $< k_A >=< k_B >= 4$. Lines are results of analytical calculation. All simulation results agree well with theory.

we can write the generating function of each layer: $G_{A0}(x) = G_{A1}(x) = e^{\lambda_A(x-1)}$ and $G_{B0}(x) = G_{B1}(x) = e^{\lambda_B(x-1)}$.

It has been proved that localized attacks cause the same effect as random attacks in ER networks.[23] Besides, as random attack is the special case of targeted attack when $\alpha = 0$, we can write the unified formula of the cascading procedure for these three attacks by considering only targeted attack.

When it comes to targeted attack, the basic idea is seeking an equivalent network $\tilde{A}$ such that after a random removal of $1-p$ fraction of nodes, the remaining network has the same distribution as that obtained by targeted attack on original network A.[24] With the equivalence described above, the generating function of network $\tilde{A}$ satisfies $G_{\tilde{A},0}(1-p+px) = G^p_{A,0}(x)$, where $G^p_{A,0}(x)$ is the degree distribution of the generating function after removing $1-p$ fraction of nodes by targeted attack. Hence, we have

$$G_{\tilde{A},0}(x) = G^p_{A,0}\left[1+\frac{1}{p}(x-1)\right] = \frac{1}{p}\sum_k \frac{\lambda^k e^{-\lambda}}{k!} t^{k^\alpha}\left[1+\frac{\tilde{p}}{p}(x-1)\right]^k, \quad (4)$$

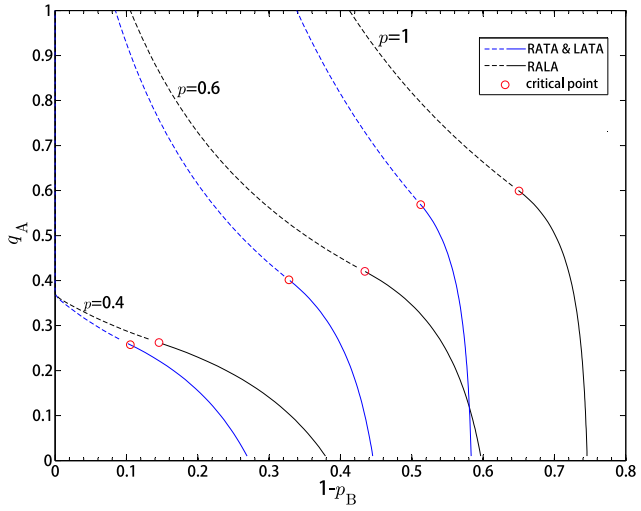

FIG. 5. The critical lines for three mixed-mode attacks on ER-ER partially interdependent networks with $q_B = 0.8$, $< k_A >=< k_B >= 4$.

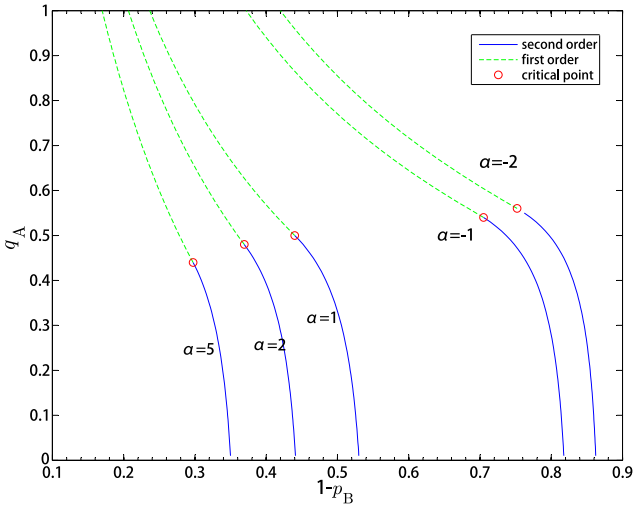

FIG. 6. The critical lines of RATA over different parameter α on ER-ER partially interdependent network with $p_B = 0.8$, $q_B = 0.8$, $< k_A >=< k_B >= 4$ from left to right, lines are $\alpha = 5, 2, 1, -1, -2$, respectively.

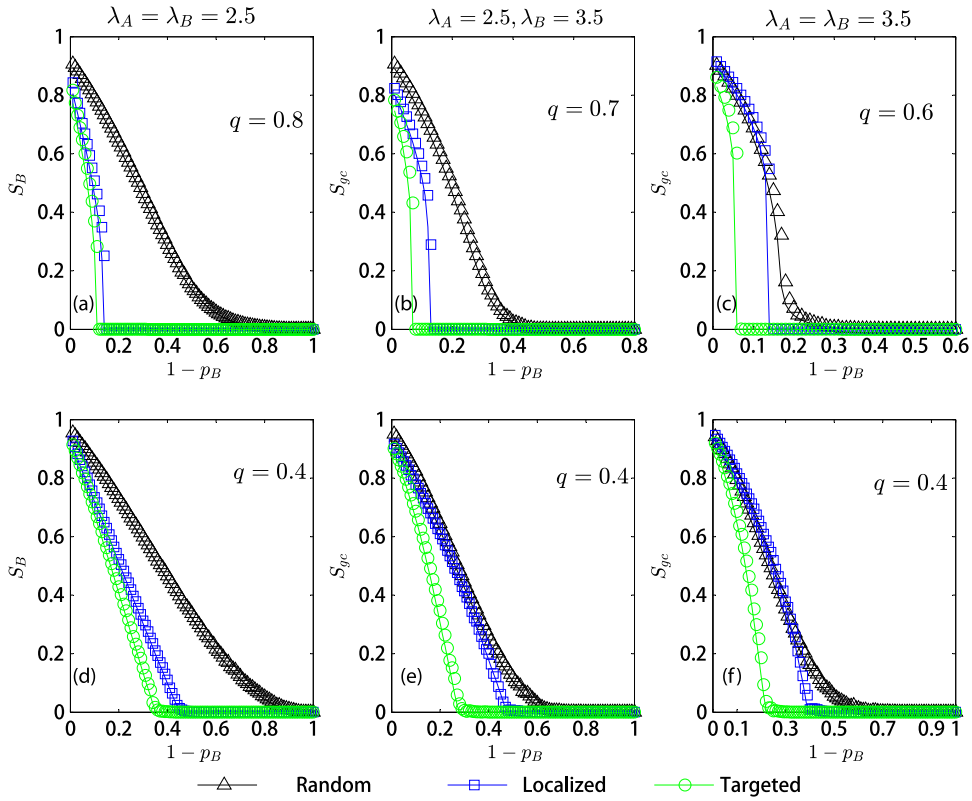

FIG. 7. The giant component of layer B on SF-SF networks with weak and strong coupling strength. The number of nodes in simulation is 10^6, and we fix $p_A = 0.9$, $q_A = q_B$. Note that simulation results agree well with theory results.

where $t = G_\alpha^{-1}(p), G_\alpha(x) = \sum p(k)x^{k^\alpha}, \tilde{p} = \frac{\sum P(k)kt^{k^\alpha}}{\sum P(k)k}$. $\alpha = 0$ is the case for random attack and localized attack in ER-ER networks.

Let $f_A(f_B)$ be the probability that layer A(B) does not have a giant component. Using Eq. (2), we can obtain f_A and f_B in the final state by solving the following equations:

$$\begin{aligned} x &= p_A[1 - q_A(1 - p_B\{1 - G_{\tilde{A},0}[1 - y(1 - f_A)]\})], \\ y &= p_B[1 - q_B(1 - p_A\{1 - G_{\tilde{B},0}[1 - x(1 - f_B)]\})], \end{aligned} \tag{5}$$

where $f_{\tilde{A}(\tilde{B})} = G_{\tilde{A}(\tilde{B}),1}\{1 - p_{A(B)}[1 - f_{\tilde{A}(\tilde{B})}]\}$. And the first and second order phase transition conditions are[14]

$$\begin{aligned} &\left.\frac{df_A(f_B)}{f_B}\right|_{p=p_I} \left.\frac{df_B(f_A)}{f_A}\right|_{p=p_I} = 1, \\ &f_A(p_{II}) = 1[f_B(p_{II}) = 1]. \end{aligned} \tag{6}$$

Submitting these conditions to Eq. (5), the critical phase transition point of the first order p_I and the second order p_{II} can be solved for a given coupling strength q.

When $\alpha = 1$, there exists a more succinct formula. Submitting $e^{\lambda(t-1)} = p$ and $\tilde{p} = pt$ into Eq. (4), we have $G_{\tilde{A}0}(x) = G_{\tilde{A}1}(x) = e^{\lambda t^2(x-1)}$. Note that for random and localized attacks, the generating function of an equivalent network is exactly the same as the original network. Hence, we write the unified analytical formula for random, localized, and targeted attacks ($\alpha = 1$) on ER-ER networks in the following way:

$$G_{\tilde{A}0}(x) = G_{\tilde{A}1}(x) = e^{\lambda t^{2\Gamma_A}(x-1)}, \tag{7}$$

where $\Gamma_A(\Gamma_B) \in \{0, 1\}$. The combined attack on interdependent networks can be coded in a binary tuple:

- $(\Gamma_A, \Gamma_B) = (0, 0)$: random attack, localized attack, or RALA.
- $(\Gamma_A, \Gamma_B) = (1, 1)$: targeted attack with $\alpha = 1$.
- $(\Gamma_A, \Gamma_B) = (0, 1)$: RATA or LATA.

Accordingly, the giant component function becomes $S_{\tilde{A}}(x) = 1 - f_{\tilde{A}}$, where $f_{\tilde{A}} = e^{\lambda_A h_A^{2\Gamma_A}(x-1)}$. Solving the system equation (5), f_A and f_B satisfy

$$\begin{aligned} f_{\tilde{A}} &= \frac{1}{q_B}\left(\frac{1 + q_B(p_A - 1)}{p_A} - \frac{\ln f_{\tilde{B}}}{\lambda_B p_A p_B h_B^{2\Gamma_B}(f_{\tilde{B}} - 1)}\right) \quad (f_{\tilde{B}} \neq 1), \\ f_{\tilde{B}} &= \frac{1}{q_A}\left(\frac{1 + q_A(p_B - 1)}{p_B} - \frac{\ln f_{\tilde{A}}}{\lambda_A p_B p_A h_A^{2\Gamma_A}(f_{\tilde{A}} - 1)}\right) \quad (f_{\tilde{A}} \neq 1). \end{aligned} \tag{8}$$

There are no restrictions on $f_{\tilde{A}}(f_{\tilde{B}})$ when $f_{\tilde{B}} = 1(f_{\tilde{A}} = 1)$.

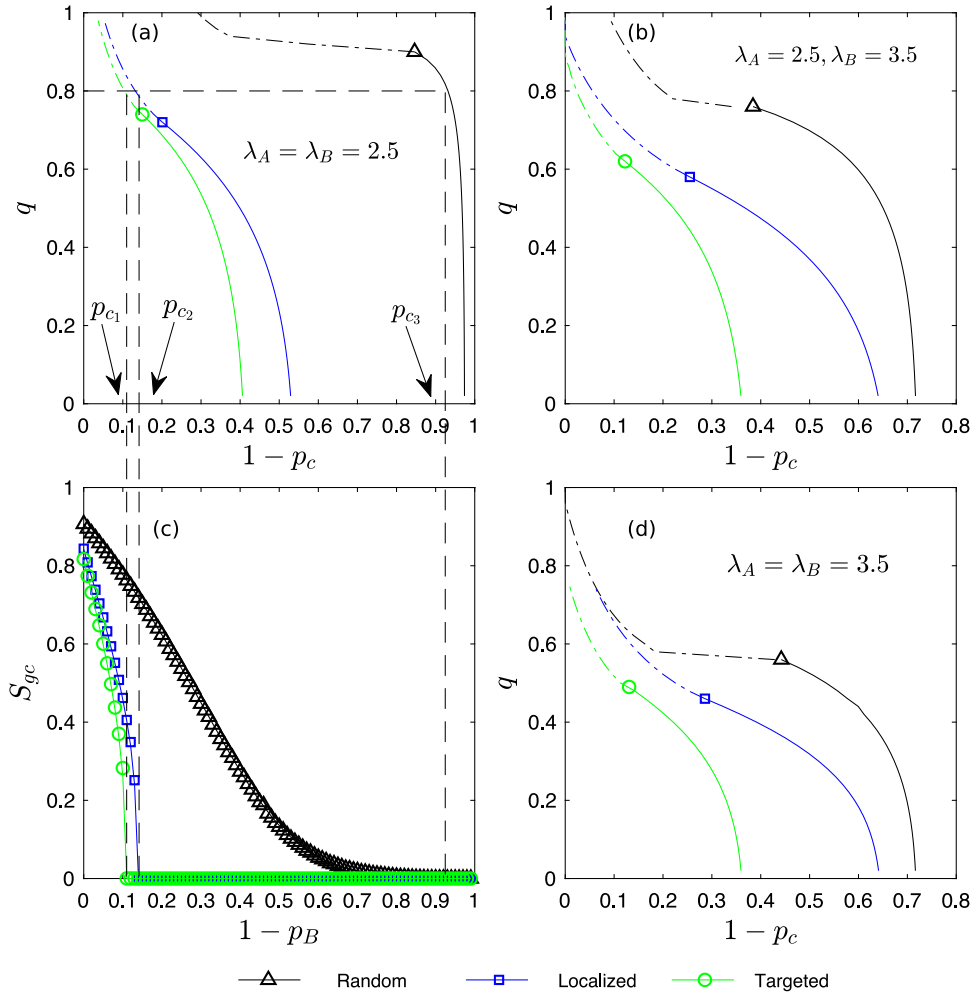

FIG. 8. The critical lines of network B on parameter space $(1 - p_B, q)$ for three single-mode attacks. In panel (a), (b), and (d), symbols (triangle-random, square-localized, circle-targeted) are the critical coupling strength q_c. Here, $q_A = q_B = q$, $p_B = 0.9$, and $p_{c_1} = 0.0684$, $p_{c_2} = 0.8682$, $p_{c_3} = 0.8961$. In panel (c), we plot the simulation and numerical results of the cascading process on SF-SF networks with $q_A = q_B = 0.8$, $p_A = 0.9$, $N = 10^6$.

A. Single-mode attack

In Fig. 2, we compare the three single-mode attacks on ER-ER partially interdependent networks with weak and strong coupling strength. The simulation results all agree well with the theory calculation obtained from Eq. (5). For a given coupling strength, the targeted attack with $\alpha = 1$ causes more serious damage than random and localized attacks. Besides, the random attack on ER-ER networks has the same effect as the localized attack, which validates our theory. Compared with the results shown in Figs. 2(a) and 2(b), the coupling strength is significantly correlated with the vulnerability of interdependent networks. The phase transition order changes from second to first when increasing the coupling strength. Consequently, strong coupling strength causes interdependent networks to be highly vulnerable even for the same attack type.

For the phase transition diagram, as shown in Fig. 3, each specific line divides the whole parameter space $(1 - p_B, q_A)$ into two regions. On the right side of the specific line, the giant component approaches zeros at the given values of q_A and p_B. While on the left side of the line, there exists a giant component on networks after cascading failure. Besides, the first order critical line (dashed) merges with the second order critical line (solid) at the critical point (p_c, q_c). Interestingly, in regions I and II, the networks behave in different phase transition orders with a given coupling strength for different attack types. The parameter α, as defined in targeted attack, has a clear effect on the attack strength.

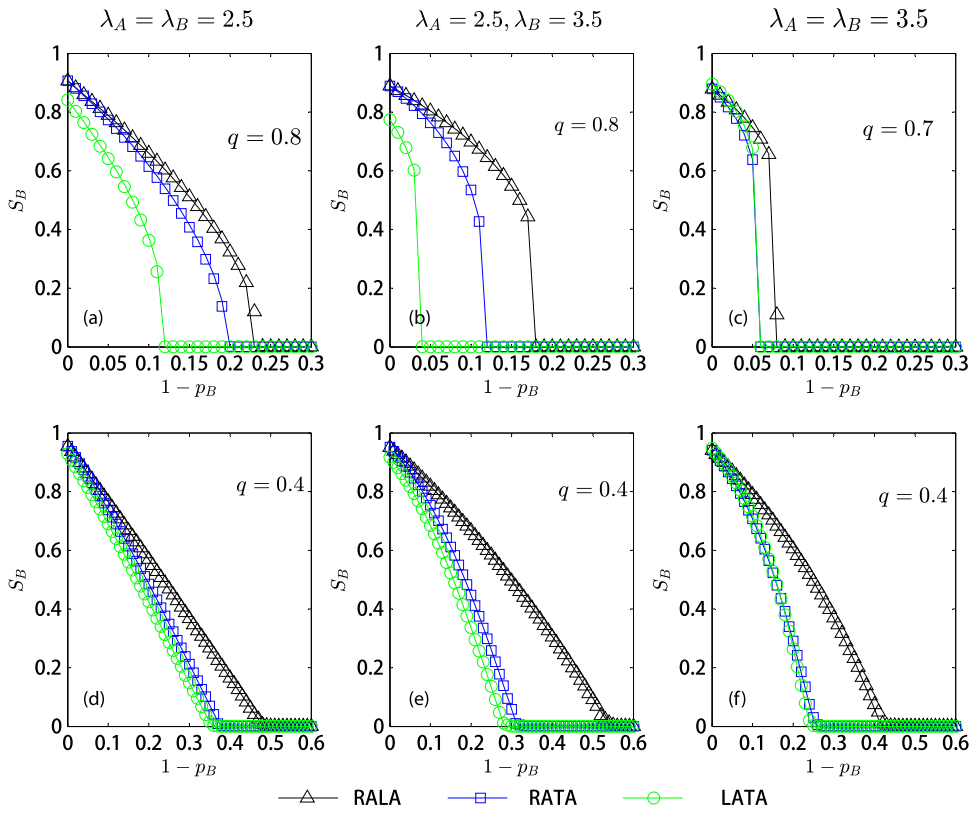

FIG. 9. The giant component of layer *B* of SF-SF networks for three mixed-mode attacks. In each simulation, the parameters are $N = 10^6, k_{min} = 2, k_{max} = 1000, q_A = q_B, p_A = 0.9$.

B. Mixed-mode attack

In this section, results for the three mixed-mode attacks on ER-ER interdependent networks are discussed. Here, we show results with $q_A = 0.54$ (weak coupling) and $q_A = 0.70$ (strong coupling) for verifying our theory. As shown in Fig. 4, the size of the giant component of networks abruptly approaches zero when the attack fraction is larger than the critical value for RATA and LATA. Likewise, a mixed-mode with targeted attack, which has prior degree information about both layers of networks, is more efficient in destroying networks than random and localized attacks. However, more information generally means consuming higher costs. Compared with the single-mode targeted attack, the RATA, with only one layer information on networks structure, is considerably efficient.

For ER-ER networks, solving Eq. (8) with $(\Gamma_A, \Gamma_B) = (0, 1), (0, 0)$, we can find the critical line of the three mixed-mode attacks over different initial attack fractions on network B. As shown in Fig. 5, with the totally distinct behavior of the critical line for RATA and RALA, the critical points (marked by red circle), however, are very close in value over each set of parameters. Besides, according to the slope of the curve, reducing the coupling strength is more conductive to improve the robustness of interdependent networks against RALA. As for RATA, it would be better to protect hub nodes to suppress the effect of targeted attack.

In Fig. 6, we plot more results of the phase transition diagram about RATA with $\alpha \in \{-2, -1, 1, 2, 5\}$. Clearly, the damage effect of RATA increases monotonically with α. Specially, when α tends to positive infinity, nodes are almost removed strictly in a descending order of degree. While α is negative, nodes with a lower degree are preferred to be removed. As shown, RATA with bigger α breakdowns networks dramatically even when the coupling strength is small. Besides, larger α significantly reduces the critical removing ratio of B. The critical coupling strength q_c, however, receives less impact.

IV. SF-SF PARTIALLY INTERDEPENDENT NETWORKS

In this section, we investigate the robustness of SF-SF partially interdependent networks. SF networks are random networks with a power law degree distribution, which is observed on many real world networks. Here, we choose the

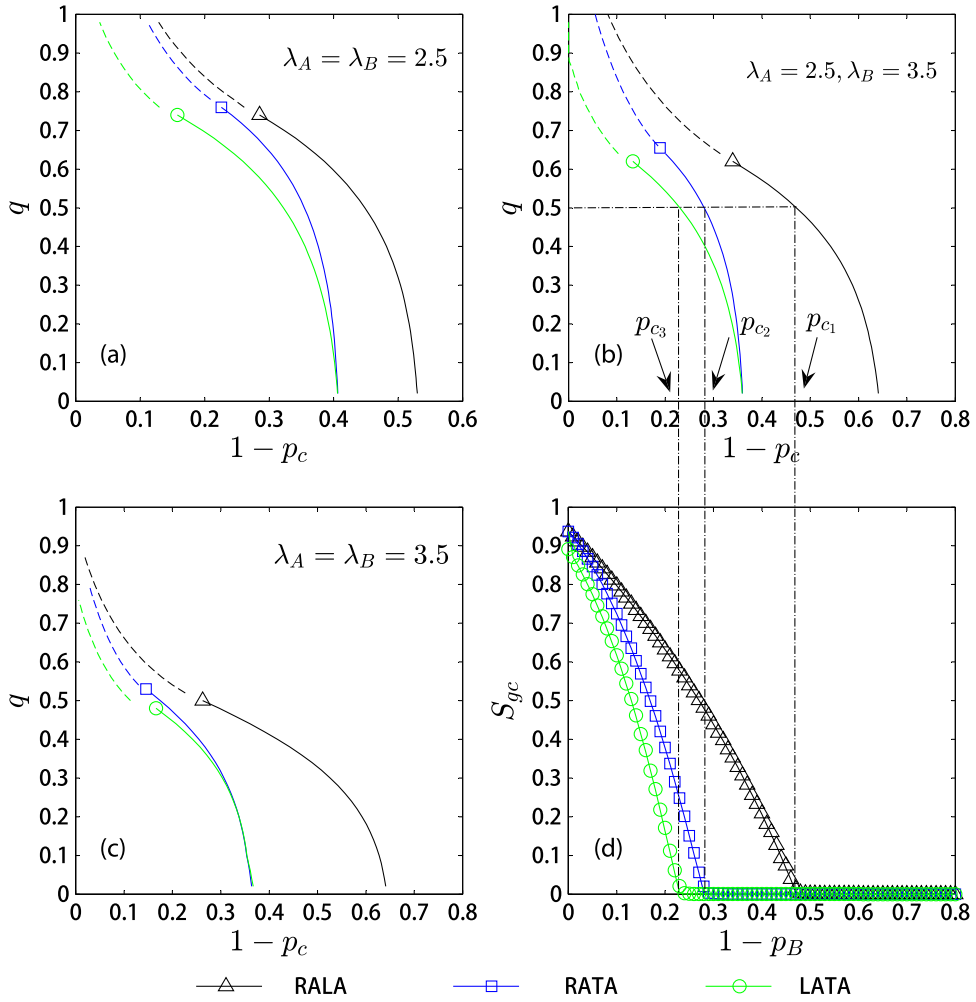

FIG. 10. The coupling strength q varies with phase transition point p_c of layer B for three mixed-mode attacks. In panel (d), we give results of the cascading procedure on SF-SF networks with $N = 10^6$, $q = 0.5$, $q_A = q_B$, $p_A = 0.9$. Note that our equations accurately predict the critical point p_c on panel (b), where $p_{c_1} = 0.5281$, $p_{c_2} = 0.7189$, $p_{c_3} = 0.7695$.

ideal power law with discrete formalism

$$p_k = \frac{k^{-\lambda}}{\sum_{k=1}^{\infty} k^{-\lambda}} = \frac{k^{-\lambda}}{\zeta(\lambda)}, \tag{9}$$

where $\zeta(\lambda)$ is the Riemann-zeta function.

Similar to the ER network, we can write the generating function for SF networks: $G_0(x) = \sum_{k=1}^{\infty} \frac{k^{-\lambda}}{\zeta(\lambda)} x^k$, $G_1(x) = \frac{G_0'(x)}{G_0'(1)}$. Submitting these to the cascading equations of the system, Eqs. (5) and (6), we can obtain the phase transition point p_c and the critical point of coupling strength q_c. For SF networks, $G_1(x)$ does not have the same form as $G_0(x)$, causing that random and localized attacks have different damage effects. Similarly, we also need the degree generating function of the equivalent network (denoting $\widehat{A}$) to solve equations for TA and LA.

For targeted attack, the generating function of the equivalent network $\widehat{A}$ is

$$G_{\widehat{A},0}(x) = \frac{1}{p_A} \sum_k \frac{k^{-\lambda_A}}{\zeta(\lambda_A)} t^{k^\alpha} \left[1 + \frac{\widetilde{p}}{p}(x-1)\right]^k, \tag{10}$$

where $t = G_\alpha^{-1}(p_A)$, $G_\alpha(x) = \sum_k \frac{k^{-\lambda}}{\zeta(\lambda)} x^{k^\alpha}$.

For localized attack, similarly, it is

$$G_{\widehat{A},0}(x) = \frac{1}{G_{A,0}(r)} G_{A,0}\left[r + \frac{G_{A,0}'(r)}{p_A G_{A,0}'(1)}(x-1)\right], \tag{11}$$

where $r = G_{B,0}^{-1}(p_A)$, $G_{A,0}(x) = \sum_k \frac{k^{-\lambda}}{\zeta(\lambda)} x^k$.

A. Single-mode attack

In Fig. 7, we fix the removing ratio of layer A with $1 - p_A = 0.1$ and vary the removing ratio p_B of network B. Each column corresponds to the power law exponent of $\lambda_A = \lambda_B = 2.5$, $\lambda_A = 2.5, \lambda_B = 3.5$, and $\lambda_A = \lambda_B = 3.5$. The first row is results of strong coupling strength. In all network configurations, damage caused by localized attack is between targeted and random attacks, where targeted attack performs the maximum damage effect among them. Besides, scale-free networks with larger λ are close to ER networks losing their SF properties. Consequently, with the increase of exponent λ, localized attack tends to be consistent with random attack except the region near the critical point. Clearly, strong coupling strength does make SF-SF interdependent networks more vulnerable. However, SF-SF interdependent networks are much robust to random attack even in a strong coupling strength compared with ER-ER networks.

Likewise, the critical point p_c and critical coupling strength q_c are calculated using the phase transition conditions by submitting related equations of SF networks into Eq. (6). In Figs. 8(a), 8(b), and 8(d), we plot critical lines of the cascading failure procedure on the SF-SF network. As shown, adjusting coupling strength q from low to high, the system undergoes the phase transition from second order (bold line, continuously) to first order (dashed line, discontinuously). And there exists a different critical point of (p_c, q_c) for all three single-mode attacks. Generally speaking, targeted attack causes the most serious damage on SF-SF networks independent of the degree exponent λ. As for the same coupling strength q, targeted attack requires the minimum removing fraction $1 - p_c$ of nodes to breakdown whole networks. However, in terms of coupling strength, localized attack always has the lowest critical coupling strength q_c (symbols), which characterizes the borderline of the system transition order. From this perspective, SF-SF networks are more vulnerable to localized attack, since networks with a lower coupling strength also suffer risks of breakdown abruptly. In Fig. 8(c), we give results of giant component size S on network B when $q_A = q_B = 0.8$. The corresponding theoretical prediction of critical point p_c is marked for the three single-mode attacks in Fig. 8(a). Clearly, theory results accurately predict the critical point $1 - p_c$ where the giant component of network B disappears on simulations.

B. Mixed-mode attack

In this section, SF-SF networks are studied under the following three mixed-mode attacks: RALA, RATA, and LATA. As shown in Fig. 9, SF-SF networks are more vulnerable for LATA (combined with localized and targeted attacks) than ER-ER networks, especially when $\lambda < 3$. Besides, RATA and LATA perform the analogous effect in the weak coupling case. In Fig. 10, the phase diagram of mixed-mode attacks on SF-SF networks is obtained by submitting the corresponding equation to the system. Obviously, LATA is the most effective way to breakdown SF-SF networks. And in terms of critical coupling strength q_c, the distinction among the three mixed-mode attacks is not significant where RATA is slightly higher than others especially with a higher degree exponent. However, when it comes to the relation between critical removing ratio $1 - p_c$ and degree exponent λ, different trends are shown among the three mixed-mode attacks. Specifically, in the strong coupling case, critical removing ratio $1 - p_c$ decreases with larger degree exponent λ for a given coupling strength, which holds for all three mixed-mode attacks; in the weak coupling case, RALA behaves the opposite manner where critical removing ratio $1 - p_c$ increases with a larger degree exponent.

V. CONCLUSIONS

Modern systems are designed in a coupling way and challenged by natural and artificial risks. In this paper, we comprehensively study cascading failures on partially interdependent networks initialized by combined attacks. Randomized, localized, and targeted attacks are considered the fundamental types. Attacks are further divided into two categories: completely executed by one of the fundamental types (single-mode) and combined by two of the fundamental types (mixed-mode). We then quantitatively study networks' robustness with a broad range of parameters. The phase diagrams are obtained by solving the transition condition equations corresponding to each combined attack. Simulation results verify the effectiveness of our theory.

In general, SF-SF networks are more robust to cascading failure compared with the ER-ER network even for combined attacks. Besides, we find that reducing the coupling strength is not an effective way to eradicate catastrophic collapse for interdependent networks especially for ER-ER networks. And targeted attacks contribute the most to the breakdown of interdependent networks on combined attacks overall. Our comprehensive numerical results can shed light on designing robust interdependence of the network structure to control cascading failure risks.

ACKNOWLEDGMENTS

This research was supported by the National Key R&D Program of China (Grant No. 2017YCF1200301) and the program of China Scholarship Council (Grant No. 201703170210).

REFERENCES

[1] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," Science **286**, 509–512 (1999).
[2] M. E. Newman, "The structure and function of complex networks," SIAM Rev. **45**, 167–256 (2003).
[3] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Resilience of the internet to random breakdowns," Phys. Rev. Lett. **85**, 4626–4628 (2000).
[4] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Breakdown of the internet under intentional attack," Phys. Rev. Lett. **86**, 3682–3685 (2001).
[5] S. Havlin, H. E. Stanley, A. Bashan, J. Gao, and D. Y. Kenett, "Percolation of interdependent network of networks," Chaos Solitons Fractals **72**, 4–19 (2015).
[6] R. Solomonoff and A. Rapoport, "Connectivity of random nets," Bull. Math. Biophys. **13**, 107–117 (1951).

[7]M. E. Newman, S. H. Strogatz, and D. J. Watts, "Random graphs with arbitrary degree distributions and their applications," Phys. Rev. E **64**, 026118 (2001).
[8]D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," Phys. Rev. Lett. **85**, 5468–5471 (2000), pRL.
[9]G. Dong, J. Fan, L. M. Shekhtman, S. Shai, R. Du, L. Tian, X. Chen, H. E. Stanley, and S. Havlin, "Resilience of networks with community structure behaves as if under an external field," Proc. Natl. Acad. Sci. U.S.A. **115**, 6911–6915 (2018).
[10]K.-M. Lee, B. Min, and K.-I. Goh, "Towards real-world complexity: An introduction to multiplex networks," Eur. Phys. J. B **88**, 1–20 (2015).
[11]Y. Yang, H. Peng, L. Li, and X. Niu, "General theory of security and a study case in internet of things," IEEE Int. Things J. **4**, 592–600 (2017).
[12]S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," IEEE Control Syst. **21**, 11–25 (2001).
[13]S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature **464**, 1025–1028 (2010).
[14]R. Parshani, "Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition," Phys. Rev. Lett. **105**, 048701 (2010).
[15]J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," Nat. Phys. **8**, 40–48 (2012).
[16]W. Li, A. Bashan, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Cascading failures in interdependent lattice networks: The critical role of the length of dependency links," Phys. Rev. Lett. **108**, 228702 (2012).
[17]J. Yuan, L. Li, H. Peng, J. Kurths, J. Xiao, and Y. Yang, "The effect of randomness for dependency map on the robustness of interdependent lattices," Chaos **26**, 013105 (2016).
[18]G. Dong, R. Du, L. Tian, and R. Liu, "Percolation on interacting networks with feedback-dependency links," Chaos **25**, 013101 (2015).
[19]A. Bashan, R. Parshani, and S. Havlin, "Percolation in networks composed of connectivity and dependency links," Phys. Rev. E **83**, 051127 (2011).
[20]R. Parshani, S. V. Buldyrev, and S. Havlin, "Critical effect of dependency groups on the function of networks," Proc. Natl. Acad. Sci. U.S.A. **108**, 1007–1010 (2011).
[21]R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," Nature **406**, 378 (2000).
[22]L. K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin, "Stability and topology of scale-free networks under attack and defense strategies," Phys. Rev. Lett. **94**, 188701 (2005).
[23]S. Shao, X. Huang, H. E. Stanley, and S. Havlin, "Percolation of localized attack on complex networks," New J. Phys. **17**, 1–11 (2014).
[24]X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," Phys. Rev. E **83**, 065101 (2011).
[25]G. Dong, J. Gao, L. Tian, R. Du, and Y. He, "Percolation of partially interdependent networks under targeted attack," Phys. Rev. E **85**, 016112 (2012).
[26]Y. Berezin, A. Bashan, M. M. Danziger, D. Li, and S. Havlin, "Localized attacks on spatially embedded networks with dependencies," Sci. Rep. **5**, 8934 (2015).
[27]D. Vaknin, M. M. Danziger, and S. Havlin, "Spreading of localized attacks in spatial multiplex networks," New J. Phys. **19**, 073037 (2017).
[28]Y. Yang, T. Nishikawa, and A. E. Motter, "Small vulnerable sets determine large network cascades in power grids," Science **358**, eaan3184 (2017).
[29]Z. Su, L. Li, H. Peng, J. Kurths, J. Xiao, and Y. Yang, "Robustness of interrelated traffic networks to cascading failures," Sci. Rep. **4**, 5413 (2014).
[30]D. Zhou, A. Bashan, R. Cohen, Y. Berezin, N. Shnerb, and S. Havlin, "Simultaneous first- and second-order percolation transitions in interdependent networks," Phys. Rev. E Stat. Nonlin. Soft Matter Phys. **90**, 012803 (2014).