PHYSICAL REVIEW E **83**, 065101(R) (2011)

Robustness of interdependent networks under targeted attack

Xuqing Huang,[1] Jianxi Gao,[1,2] Sergey V. Buldyrev,[3] Shlomo Havlin,[4] and H. Eugene Stanley[1]
[1]*Center for Polymer Studies and Department of Physics, Boston University, Boston, Massachusetts 02215, USA*
[2]*Department of Automation, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai, 200240, People's Republic of China*
[3]*Department of Physics, Yeshiva University, New York, New York 10033, USA*
[4]*Minerva Center and Department of Physics, Bar-Ilan University, 52900 Ramat-Gan, Israel*
(Received 11 October 2010; revised manuscript received 9 March 2011; published 27 June 2011)

When an initial failure of nodes occurs in interdependent networks, a cascade of failure between the networks occurs. Earlier studies focused on random initial failures. Here we study the robustness of interdependent networks under targeted attack on high or low degree nodes. We introduce a general technique which maps the *targeted-attack* problem in interdependent networks to the *random-attack* problem in a transformed pair of interdependent networks. We find that when the highly connected nodes are protected and have lower probability to fail, in contrast to single scale-free (SF) networks where the percolation threshold $p_c = 0$, coupled SF networks are significantly more vulnerable with p_c significantly larger than zero. The result implies that interdependent networks are difficult to defend by strategies such as protecting the high degree nodes that have been found useful to significantly improve robustness of single networks.

DOI: 10.1103/PhysRevE.83.065101 PACS number(s): 89.75.Hc, 64.60.ah, 89.75.Fb

Modern systems due to technological progress are becoming more and more mutually coupled and depend on each other to provide proper functionality [1–3]. For example, blackouts are usually caused by cascading failures between the power grid and its communication support system [3]. While cascade of failures in one network, e.g., overload failure, can cause dramatic damage to a system [4,5], social disruptions caused by recent disasters, ranging from hurricanes to large-scale power outages and terrorist attacks, have shown that the most dangerous vulnerability is hiding in the many interdependencies across different networks [6]. The question of robustness of interdependent networks has recently become of interest [7–10]. In interdependent networks, nodes from one network depend on nodes from another network and vice versa. Consequently, when nodes from one network fail they cause nodes in the other network to fail, too. When some initial failure of nodes happens, this may trigger a recursive process of cascading failures that can completely fragment both networks.

Recently, a theoretical framework was developed [7] to study the process of cascading failures in interdependent network caused by *random* initial failure of nodes. They show that due to the coupling between networks, interdependent networks are extremely vulnerable to random failure. However, when we consider real scenarios, initial failure is mostly not random. It may be due to a *targeted attack* on important hubs (nodes with high degree). It can also occur to low degree nodes because important hubs are purposely defended, e.g., in internet networks, heavily connected hubs are purposely more secured. Indeed, it was shown that targeted attacks on high degree nodes [11–16] or high betweenness nodes [17,18] in *single* networks have a dramatic effect on their robustness. The question of robustness of *interdependent* networks under targeted attack or defense has not been addressed.

In this Rapid Communication, we develop a mathematical framework for understanding the robustness of interdependent networks under an initial targeted attack which depends on degree of nodes. The framework is based on a general technique we develop to solve targeted-attack problems in networks by mapping them to random-attack problems. A value $W_\alpha(k_i)$ is assigned to each node, which represents the probability that a node i with k_i links is initially attacked and become inactive. We focus on the family of functions [14]

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

When $\alpha > 0$, nodes with a higher degree are more vulnerable for the intentional attack, while for $\alpha < 0$, nodes with a higher degree are defended and so have lower probability to fail. The case $\alpha = 0$, $W_0 = \frac{1}{N}$, represents the random removal of nodes [7,19], and the case $\alpha \to \infty$ represents the targeted-attack case where nodes are removed strictly in the order from high degree to low degree. For the $\alpha < 0$ case, nodes with zero degree should be removed before analysis begins. An important special case $\alpha = 1$ corresponds to the acquaintance immunization strategy [20].

Our model consists of two networks, A and B, with the same number of nodes N. The N nodes in each network are connected to nodes in the other network by bidirectional dependency links, thereby establishing a one-to-one correspondence. The functioning of a node in network A depends on the functioning of the corresponding node in network B and vice versa. Within each network, the nodes are randomly connected with degree distributions $P_A(k)$ and $P_B(k)$, respectively. We begin by studying the situation where only network A is attacked. We initially remove a fraction, $1 - p$ of nodes from network A selecting them with probability $W_\alpha(k_i)$ [Eq. (1)] and remove all the links that connect to those removed nodes. As nodes and links are sequentially removed, network A begins to fragment into connected components. Nodes that are not connected to the giant component are considered inactive and are removed. Owing to the dependence between the networks, all the nodes in network B that are connected to the removed nodes in network A are then also removed. Network B also begins to fragment into connected components and only the nodes in the giant component are kept. Then network B spreads damage back to network A. The damage is spread between network A and B, back and

forth until they completely fragment or arrive to a mutually connected giant component and no further removal of nodes and links occurs.

The main idea of our approach is to find an equivalent network A', such that the *targeted*-attack problem on interdependent networks A and B can be solved as a *random*-attack problem on interdependent networks A' and B. We start by finding the degree distribution $P_p(k)$ of the remaining nodes in network A after removing, according to Eq. (1), $(1-p)$ fraction of nodes but keeping the edges of the remaining nodes which lead to the removed nodes. Let $A_p(k)$ be the number of nodes with degree k,

$$P_p(k) = \frac{A_p(k)}{pN}. \tag{2}$$

When another node is removed, $A_p(k)$ changes as

$$A_{(p-1/N)}(k) = A_p(k) - \frac{P_p(k)k^\alpha}{\langle k^\alpha(p)\rangle}, \tag{3}$$

where $\langle k^\alpha(p)\rangle \equiv \sum P_p(k)k^\alpha$. In the limit of $N \to \infty$, Eq. (3) can be presented in terms of derivative of $A_p(k)$ with respect to p,

$$\frac{dA_p(k)}{dp} = N\frac{P_p(k)k^\alpha}{\langle k^\alpha(p)\rangle}. \tag{4}$$

Differentiating Eq. (2) with respect to p and using Eq. (4), we obtain

$$-p\frac{dP_p(k)}{dp} = P_p(k) - \frac{P_p(k)k^\alpha}{\langle k^\alpha(p)\rangle}, \tag{5}$$

which is exact for $N \to \infty$. In order to solve Eq. (5), we define a function $G_\alpha(x) \equiv \sum_k P(k)x^{k^\alpha}$, and following Ref. [21] introduce a new variable $t \equiv G_\alpha^{-1}(p)$. We find by direct differentiation that

$$P_p(k) = P(k)\frac{t^{k^\alpha}}{G_\alpha(t)} = \frac{1}{p}P(k)t^{k^\alpha}, \tag{6}$$

$$\langle k^\alpha(p)\rangle = \frac{tG'_\alpha(t)}{G_\alpha(t)}, \tag{7}$$

satisfy Eq. (5). Thus the generating function of $P_p(k)$ is

$$G_{Ab}(x) \equiv \sum_k P_p(k)x^k = \frac{1}{p}\sum_k P(k)t^{k^\alpha}x^k. \tag{8}$$

Because network A is randomly connected, the probability for an edge to end at a remaining node is equal to the ratio of the number of edges emanating from the remaining nodes to the total number of edges emanating from all the nodes of the original network:

$$\tilde{p} \equiv \frac{pN\langle k(p)\rangle}{N\langle k\rangle} = \frac{\sum_k P(k)kt^{k^\alpha}}{\sum_k P(k)k}, \tag{9}$$

where $\langle k\rangle$ is the average degree of the original network A, and $\langle k(p)\rangle$ is the average degree of remaining nodes. Removing the edges which end at the deleted nodes of a randomly connected network is equivalent to randomly removing a $(1-\tilde{p})$ fraction of edges of the remaining nodes. Using the same approach as in Ref. [22], one can show that the generating function of the remaining nodes after random removal of $(1-\tilde{p})$ fraction of edges is equal to

$$G_{Ac}(x) \equiv G_{Ab}(1-\tilde{p}+\tilde{p}x). \tag{10}$$

Notice that Eq. (10) is the generating function of the remaining nodes in network A after a targeted attack. The only difference in the cascading process under a *targeted* attack from the case under a *random* attack is the first stage where the initial attack is exerted on network A. If we find a network A' with generating function $\tilde{G}_{A0}(x)$, such that after a random attack which removes $(1-p)$ fraction of nodes, the generating function of the remaining nodes in A' is the same as $G_{Ac}(x)$, then the targeted-attack problem on interdependent networks A and B can be solved as a random-attack problem on interdependent networks A' and B. We find $\tilde{G}_{A0}(x)$ by solving the equation $\tilde{G}_{A0}(1-p+px) = G_{Ac}(x)$ and from Eq. (10),

$$\tilde{G}_{A0}(x) = G_{Ab}\left(1+\frac{\tilde{p}}{p}(x-1)\right). \tag{11}$$

Up to now, we have mapped the problem of cascade of failures of nodes in interdependent networks caused by an initial *targeted* attack to the problem of a *random* attack. Since the derivation of equations only depends on the generating function of network A, this approach can be generally applied to study both single networks with dependency links [23] and other more general interdependent network models, as long as the nodes in those networks are randomly connected.

Next we apply the framework developed in Ref. [7]. We introduce a function $g_A(p) = 1-\tilde{G}_{A0}[1-p(1-f_A)]$, where f_A is a function of p that satisfies the transcendental equation $f_A = \tilde{G}_{A1}[1-p(1-f_A)]$. Analogous equations exist for network B. As the interdependent networks achieve a mutually connected giant component, the fraction of nodes left in the giant component is p_∞, which can be found by solving a system of equations

$$x = pg_A(y), \quad y = pg_B(x), \tag{12}$$

where the two unknown variables x and y yield $p_\infty = xg_B(x) = yg_A(y)$. Eliminating y from these equations, we obtain a single equation

$$x = pg_A[pg_B(x)]. \tag{13}$$

The critical case ($p = p_c$) emerges when both sides of this equation have equal derivatives,

$$1 = p^2\frac{dg_A}{dx}[pg_B(x)]\frac{dg_B}{dx}(x)|_{x=x_c,p=p_c}. \tag{14}$$

which, together with Eq. (13), yields the solution for p_c and the critical size of the giant mutually connected component, $p_\infty(p_c) = x_c g_B(x_c)$. In general, p_c and x_c can be found numerically without an explicit expression.

We now analyze the specific classes of Erdös-Rényi (ER) [24,25] and scale-free (SF) [26–29] networks. Critical thresholds p_c of networks obtained by solving Eqs. (13) and (14) are presented in Fig. 1. Remarkably, while p_c for a single SF network approaches to 0 quickly when α becomes zero or negative (see also Ref. [14]), p_c for interdependent SF networks is nonzero for the entire range of α [Fig. 1(a)]. This follows from the fact that failure of the least connected nodes

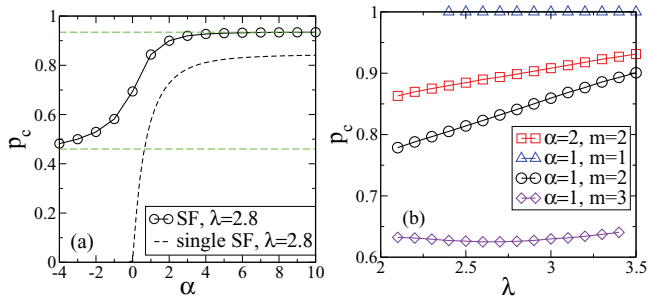

FIG. 1. (Color online) (a) Dependence of p_c on α for single and interdependent SF networks with a lower cutoff of degree $m = 2$. The horizontal lines represent the upper and lower limits of p_c as $\alpha = \pm\infty$. The curved dashed line represents p_c for single SF networks. (b) Threshold p_c vs λ for interdependent SF networks with different m and α.

in one network may lead to failure of well connected nodes in the other network, which makes interdependent networks significantly more difficult to protect compared to a single network. Increasing degree correlation between interdependent nodes will increase the robustness of interdependent networks. However, as shown in Ref. [30], even when the interdependent networks have the highest possible degree-degree correlation, the system of interdependent networks is still significantly more vulnerable than a single network and the transition is of the first-order type, if the degree distribution has a finite second moment. Figure 1(b) shows that p_c of interdependent SF networks is sensitive to a minimum possible degree but not that sensitive to λ. As $m = 1$, the interdependent SF networks become extremely vulnerable.

Simplified forms for $G_{Ab}(x)$, $G_{Ac}(x)$, and $\tilde{G}_{A0}(x)$ from Eqs. (8), (10), and (11) exist when $\alpha = 1$,

$$G_{Ab}(x) = \frac{1}{p}\sum_k P(k)t^k x^k = \frac{1}{p}G_{A0}(tx), \tag{15}$$

$$G_{Ac}(x) = \frac{1}{p}G_{A0}(t(1-\tilde{p}+\tilde{p}x)), \tag{16}$$

$$\tilde{G}_{A0}(x) = \frac{1}{p}G_{A0}\left(\frac{\tilde{p}}{p}t(x-1)+t\right). \tag{17}$$

where $G_{A0}(x)$ is the original generating function of network A, $t = G_{A0}^{-1}(p)$ and $\tilde{p} = \frac{G'_{A0}(t)}{G'_{A0}(1)}t$.

Explicit solutions of percolation quantities exist for the case of interdependent Erdös-Rényi networks, when $\alpha = 1$ and both of the two networks are initially attacked simultaneously. The two networks originally have generating functions $G_{A0}(x)$ and $G_{B0}(x)$. Initially, $(1 - p_1)$ and $(1 - p_2)$ fraction of nodes are targeted [according to Eq. (1) and] and removed from networks A and B, respectively. Similarly, we start by finding the equivalent networks A' and B' such that random removal of $(1 - p_1p_2)$ fraction of nodes on both networks A' and B' has the same effect as when $(1 - p_1)$ and $(1 - p_2)$ fractions of nodes are intentionally removed from network A and network B, respectively. After the same consideration as discussed before, we find the generating function of network A',

$$\tilde{G}_{A0}(x) = \frac{1}{p_1}G_{A0}\left(\frac{\tilde{p}_1}{p_1}t_1(x-1)+t_1\right). \tag{18}$$

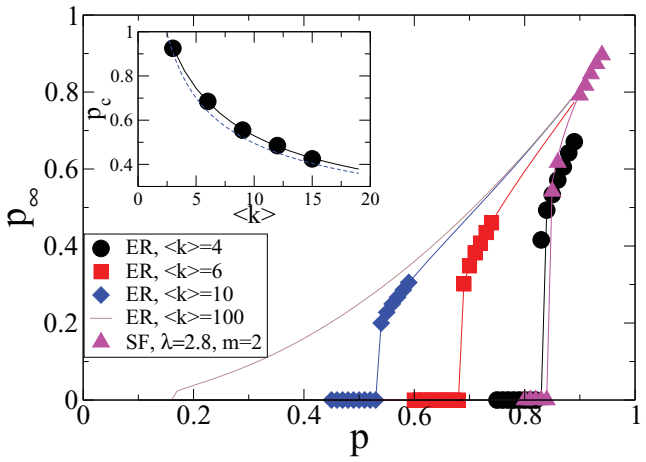

FIG. 2. (Color online) Values of p_∞ vs p for theory and simulation. All results are for $\alpha = 1$. The symbols represent simulation data ($N = 10^6$ nodes). The solid lines are theoretical predictions based on Eq. (21) for ER networks and numerical solution of Eqs. (13) and (17) for SF networks. For the interdependent ER network case, both networks are under an initial targeted attack. For the interdependent SF network case, only one network is under an initial targeted attack. Inset: Values of p_c vs average degree of ER networks with $\alpha = 1$. The symbols represent simulation data, while the solid line is the theory, Eq. (22). The dashed line is p_c under random attack with $\alpha = 0$.

where $t_1 \equiv G_{A0}^{-1}(p_1)$, $\tilde{p}_1 \equiv t_1\frac{G'_{A0}(t_1)}{G'_{A0}(1)}$. The same holds for network B'.

For ER networks, the generating function is $G_0(x) = e^{\langle k\rangle(x-1)}$ [22], so $t_1 = \frac{\ln(p_1)}{\langle k\rangle_1} + 1$, $t_2 = \frac{\ln(p_2)}{\langle k\rangle_2} + 1$, $\tilde{G}_{A0}(x) = \tilde{G}_{A1}(x) = e^{\langle k\rangle_1 t_1^2(x-1)}$, and $\tilde{G}_{B0}(x) = \tilde{G}_{B1}(x) = e^{\langle k\rangle_2 t_2^2(x-1)}$. From Eq. (12),

$$\begin{aligned} x &= p_1p_2g_A(y) = p_1p_2(1-f_A), \\ y &= p_1p_2g_B(x) = p_1p_2(1-f_B), \end{aligned} \tag{19}$$

where

$$f_A = e^{\langle k\rangle_1 t_1^2 y(f_A-1)}, \quad f_B = e^{\langle k\rangle_2 t_2^2 x(f_B-1)}. \tag{20}$$

In the case $\langle k\rangle_1 = \langle k\rangle_2 = \langle k\rangle$ and $p_1 = p_2 = p$, we find that

$$p_\infty = p^2(1 - e^{-\langle k\rangle t^2 p_\infty})^2, \tag{21}$$

where $t_1 = t_2 \equiv t = \frac{\ln(p)}{\langle k\rangle} + 1$, and p_c satisfies the relation

$$\langle k\rangle p_c^2 t_c^2 = 2.4554, \tag{22}$$

with $t_c = \frac{\ln(p_c)}{\langle k\rangle} + 1$. Figure 2 shows that simulations confirm well the theory for interdependent ER networks. If only *one* network of the interdependent networks is *randomly* attacked, Ref. [7] shows that $p_c = 2.4554/\langle k\rangle$. In Eq. (22), the term p_c^2 is since we are initially attacking both interdependent networks simultaneously. Indeed, for the case of a *random* initial attack on both networks, we obtain $\langle k\rangle p_c^2 = 2.4554$. The factor t_c in Eq. (22) reflects the effect of a targeted attack. Here for $\alpha = 1$, $t_c = \frac{\ln(p_c)}{\langle k\rangle} + 1$ is always smaller than 1, which increases p_c compared to the random-attack case, shown in inset of Fig. 2.

For interdependent ER networks, the effect of a targeted attack is not significant, but for interdependent SF networks, the effect is substantial [Fig. 1(a)].

The mapping method we develop in this Rapid Communication is applicable for randomly connected networks. In an infinitely large network with a finite second moment of degree distribution, the probability of the formation of parallel edges, connecting the same pair of nodes and looped edges ending at the same node, is negligible and no degree-degree correlations are present. For SF networks with $\lambda \leqslant 3$, it is impossible to construct a randomly connected network with a negligible fraction of self-loops and parallel edges [31]. SF networks without self-loops and parallel links have negative (disassortative) degree-degree correlations from the start [21], and for such networks our theory is an approximation. In Fig. 2, we show that the theoretical p_∞ obtained by numerical calculation confirms well the simulation results for interdependent SF networks with $\lambda = 2.8$, which allows self-loops and parallel links.

In summary, we developed a theoretical framework for understanding the robustness of interdependent networks under targeted attacks on specific degree nodes. We show that targeted-attack problems can be mapped to random-attack problems by transforming the networks which are under initial attack. It provides a routine method to study the degree-based targeted-attack problems in both single networks with dependency links [23,32] and other general randomly connected and uncorrelated interdependent networks, i.e., (i) the case of three or more interdependent networks, (ii) the case of partially coupled interdependent networks [10], and (iii) the case in which a node from network A can depend on more than one node from network B [33]. By applying the method, we find that in contrast to single networks, when the highly connected nodes are defended ($\alpha < 0$), the percolation threshold p_c has a finite nonzero value which is significantly larger than zero. The study implies that interdependent networks are difficult to defend by strategies such as protecting the high degree nodes that have been found useful to significantly improve the robustness of single networks.

ACKNOWLEDGMENTS

S. V. B. acknowledges the partial support of this research through the Dr. Bernard W. Gamson Computational Science Center at Yeshiva College. J. G. thanks the Doctoral visiting scholar programme of SJTU, the Shanghai Key Basic Research Project and the National Natural Science Foundation of China for support. S. H. acknowledges support from the Israel Science Foundation, the DFG and the Epiwork EU project. We thank the DTRA and the Office of Naval Research for support.

[1] J. C. Laprie, K. Kanoun, and M. Kaniche, Lect. Notes Comput. Sci. **54**, 4680 (2007).
[2] S. Panzieri and R. Setola, Int. J. Modelling, Identication and Control **3**, 69 (2008).
[3] V. Rosato *et al*., Int. J. Crit. Infrastruct. **4**, 63 (2008).
[4] A. E. Motter and Ying-Cheng Lai, Phys. Rev. E **66**, 065102 (2002).
[5] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, and D. Helbing, Phys. Rev. Lett. **100**, 218701 (2008).
[6] S. E. Chang, The Bridge **39**, 36 (2009); S. M. Rinaldi *et al*., IEEE Control Syst. Mag. **21**, 11 (2001).
[7] S. V. Buldyrev *et al*., Nature (London) **464**, 1025 (2010).
[8] A. Vespignani, Nature (London) **464**, 984 (2010).
[9] E. A. Leicht and M. D'Souza, e-print arXiv:0907.0894v1.
[10] R. Parshani, S. V. Buldyrev, and S. Havlin, Phys. Rev. Lett. **105**, 048701 (2010).
[11] R. Albert, H. Jeong, and A. L. Barabási, Nature (London) **406**, 378 (2000).
[12] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).
[13] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).
[14] L. K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, and S. Havlin Phys. Rev. Lett. **94**, 188701 (2005).
[15] A. A. Moreira, J. S Andrade, H. J. Herrmann, and J. O. Indekeu Phys. Rev. Lett. **102**, 018701 (2009).
[16] A. Annibale, A. Coolen, and G. Bianconi, J. Phys. A **43**, 395001 (2010).
[17] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Phys. Rev. E **65**, 056109 (2002).
[18] C. M. Schneider *et al*., Proc. Natl. Acad. Sci. USA **108**, 3838 (2011).
[19] R. Cohen *et al*., Phys. Rev. Lett. **85**, 4626 (2000).
[20] R. Cohen *et al*., Phys. Rev. Lett. **91**, 247901 (2003).
[21] J. Shao, S. V. Buldyrev, L. A. Braunstein, S. Havlin, and H. E. Stanley, Phys. Rev. E **80**, 036105 (2009).
[22] M. E. J. Newman, Phys. Rev. E **66**, 016128 (2002).
[23] R. Parshani *et al*., Proc. Natl. Acad. Sci. USA **108**, 1007 (2011).
[24] P. Erdös and A. Rényi, Publ. Math. (Debrecen) **6**, 290 (1959); Publ. Math. Inst. Hung. Acad. Sci. **5**, 17 (1960).
[25] B. Bollobás, *Random Graphs* (Academic, London, 1985).
[26] A. L. Barabási and R. Albert, Science **286**, 509 (1999).
[27] R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002).
[28] G. Caldarelli and A. Vespignani, *Large Scale Structure and Dynamics of Complex Webs* (World Scientific, Singapore, 2007).
[29] S. Havlin and R. Cohen, *Complex Networks: Structure, Robustness and Function* (Cambridge University Press, Cambridge, UK, 2010).
[30] S. Buldyrev *et al*., Phys. Rev. E **83**, 016112 (2011).
[31] M. Boguñá, R. Pastor-Satorras, and A. Vespignani, Eur. Phys. J. B **38**, 205 (2004).
[32] A. Bashan *et al*., Phys. Rev. E **83**, 051127 (2011).
[33] Jia Shao *et al*., Phys. Rev. E **83**, 036116 (2011).