Spreading of localized attacks on spatial multiplex networks with a community structure

Dana Vaknin,[1] Bnaya Gross,[1] Sergey V. Buldyrev,[2] and Shlomo Havlin[1]
[1]*Department of Physics, Bar-Ilan University, Ramat Gan 5290002, Israel*
[2]*Department of Physics, Yeshiva University, New York 10033, USA*

(Received 16 December 2019; accepted 8 September 2020; published 1 October 2020)

We study the effect of localized attacks on a multiplex network, where each layer is a network of communities embedded in space. We assume that nodes are densely connected within a community and sparsely connected to the nodes in the neighboring communities. To investigate percolation processes in this realistic system we develop an analytical scheme, applying the finite-element method. We find, both by simulation and theory, that in many cases there is a critical size of localized damage above which it will spread and the entire system will collapse. In addition, we show that for a constant number of links, networks with less connectivity between communities are surprisingly more robust.

DOI: 10.1103/PhysRevResearch.2.043005

I. INTRODUCTION

In recent years, due to the advances in technology, many systems have become more and more integrated and interdependent. This interdependence can cause a spread of damages, and lead to a cascade of failures and even entire system collapse. Therefore, many studies have been carried out to analyze cascading failures in interdependent networks [1–11]. Many of these studies have focused on the multiplex network model, which is an important example of an interdependent network where the same nodes are linked by different layers [12–15]. Further, in many real systems such as power grids and transportation systems, the links are of typical relatively short length due to the embedding in space [16]. In such spatial systems, the initial failures or attacks can be localized to a specific region. Recent studies show that in different cases of spatial interdependent networks, localized attacks are significantly more damaging than random attacks [17–20]. In addition, many real networks have a modular structure [21], such as biological networks [22,23] and many infrastructure systems [24,25]. Therefore, recent studies have explored and compared the robustness of individual and interdependent modular non-spatial systems [26–29]. Our study combines for the first time, three ubiquitous features of real complex systems—interdependence, spatiality and modularity.

Here, we analyze and predict the resilience of spatial multiplex networks with modular structure under localized attacks, by developing tools based on percolation theory [30–33]. Examples of systems that provide motivation for our model are infrastructure networks [34,35], ecological systems [36], and financial networks [37]. Specifically, in the infrastructure example, each layer describes different infrastructure in a country, such as power grids, communications networks, water supply, etc. The different infrastructures are dependent on each other, and in addition, each layer has high connections within the cities and a few long connections between nearby cities. We focus on localized failures because of two main reasons. First, a localized damage is a realistic scenario (due to flood or earthquake), and second, in such systems, a finite number of local failures concentrated in the same area might spread the damage throughout the system and cause significant damage and even to a complete system collapse.

II. MODEL

Our model is generated as a multiplex system with spatial and community properties (see Fig. 1). A multiplex network is a single network with at least two kinds of connectivity links. We assume here that the two types of links serve for two different functions, such as transportation and communication. In fact, a multiplex network with two kinds of connectivity links (for instance) can be regarded as a special case of interdependent networks in which two layers have the same number of nodes, and every node in one layer has only one interdependent link with a single node in the other layer. For a node to remain functional in the multiplex, it must be connected to the giant component in both layers. This reflects the assumption that, in order for a node in the system to function, it requires both resources provided by the two layers. The condition of belonging to a giant component can be replaced by a condition of belonging to a cluster of sufficiently large size [38].

For simplicity and without loss of generalization, our multiplex model is composed of two layers in which the nodes are placed at sites of a square lattice of size $L \times L$. Each layer is constructed as $m \times m$ Erdős-Rényi (ER) networks (communities) of size $\zeta \times \zeta$, where $\zeta = L/m$, which are tiled and connected to each other as a square lattice (see Fig. 1).

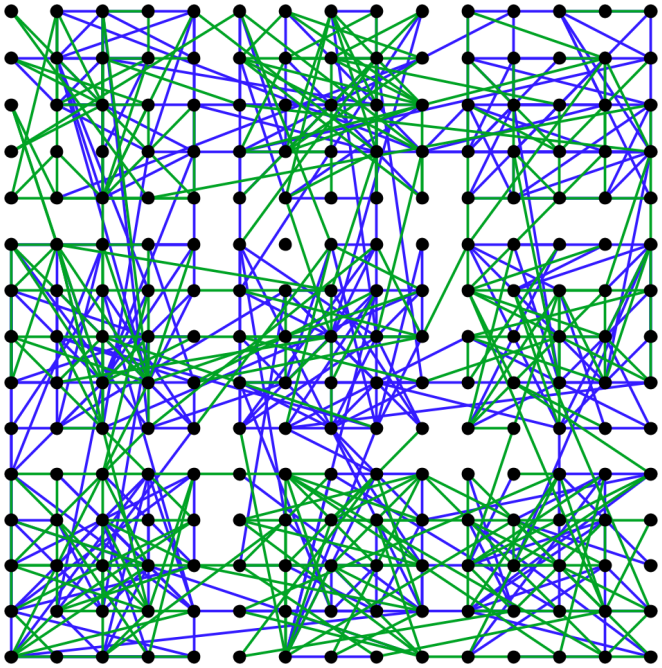

FIG. 1. A schematic representation of the model. The nodes are at the lattice sites of a two-dimensional square lattice of size $L \times L$ with $L = 15$. The system is constructed as $m \times m$ Erdős-Rényi (ER) networks. Here $m = 3$, where each ER network is of size $\zeta \times \zeta$ with $\zeta = 5$. The green and blue lines represent the links in the first and second layer of the multiplex and are constructed independently of each other. In our simulations we set periodic boundary conditions, not shown for clarity.

We assume that *intralinks* connect pairs of nodes in the same community, while *interlinks* connect two nodes belonging to two distinct neighboring communities. Each node has a degree k_{inter} of interlinks and a degree k_{intra} of intralinks, and the total degree is set to be $k_{\text{total}} = k_{\text{inter}} + k_{\text{intra}}$. We assume that k_{inter} and k_{intra} are independent random variables taken from two different degree distributions which are characterized by average degrees $\langle k_{\text{inter}} \rangle$ and $\langle k_{\text{intra}} \rangle$, respectively. In addition, the heterogeneity of the system is specified by the interconnectivity parameter $\alpha = \langle k_{\text{inter}} \rangle / \langle k_{\text{total}} \rangle$. It should be noted that the homogeneous case (without communities) has been previously studied for both single-layer [39,40] and multilayer [20,41] networks. In that model, all links have a characteristic length ζ with no distinction between inter- and intralinks and therefore representing homogeneous systems. In contrast, the present model can describe systems with a spatial structure of communities, where the heterogeneity of the system is controlled by the α parameter. Thus, this model enables us to expand the previous model to a more general and realistic one for systems such as interconnected cities. It is important to note that the model described in this paper provides qualitative description of the abovementioned realistic systems and does not purport to be an accurate description of them.

III. THEORY AND SIMULATION RESULTS

Here we develop a theoretical framework for understanding the cascading process that follows an initial attack, for a general case of a multiplex network with two layers. The constraints are that each layer has a spatial structure of communities which are connected in the form of an arbitrary graph including a lattice.

In the cascading process, at first we remove all nodes that are not in the giant component (GC) of the first layer. Then, from the set of the remaining nodes, we remove all the nodes that are not in the GC of the second layer. We repeat these two steps until there are no nodes to remove, and we are left with the mutual giant component (MGC). The existence of a MGC of size $O(N)$, where N is the number of nodes in the network, expresses the functionality of the system.

In order to analytically obtain the size of the MGC, we use a method similar to a finite-element approach [42] in which we introduce nonlinear equations for each community and for each intercommunity link, treating the entire system as a network of communities. We begin with deriving equations for the GC size of a single layer after an attack (i.e., nodes removal). We assume that the number of links $k_{\nu,i,j}$ linking any node ν in community i to nodes in community j is statistically independent from number $k_{\nu,i,\ell}$, linking node ν to any other community ℓ. These numbers are randomly taken from given degree distributions $P_{i,j}(k)$. We define the generating functions of these distributions as $G_{i,j}(x) = \sum_{k=0}^{\infty} P_{i,j}(k) x^k$, and we define the generating functions of the excess degree distribution [43] as $H_{i,j}(x) = \sum_{k=0}^{\infty} \frac{P_{i,j}(k+1)(k+1)}{\langle k_{i,j} \rangle} x^k$, where $\langle k_{i,j} \rangle$ are the average degrees of distributions $P_{i,j}(k)$.

We define $f_{i,j}$ as the probability that a randomly selected link, which passes from a node in community i to a node in community j, does not lead to the GC.

Therefore, $1 - f_{i,j}$ is the probability that the node we reach, by the incoming link, survived the attack and has at least one outgoing link which leads to the GC. When calculating the probability that an outgoing link of the reached node is not connected to the GC, we distinguish between two cases. In the case of an outgoing link that goes back to community i, we use the generating function $H_{j,i}$ since one of the links leading from the reached node to community i is used by the incoming link. In the complementary case, we use the generating function $G_{j,\ell}$. Thus, when defining p_j as the fraction of nodes that survived in community j as a result of an attack, $f_{i,j}$ fulfill the equations

$$1 - f_{i,j} = p_j \left[1 - H_{j,i}(f_{j,i}) \prod_{\ell \neq i} G_{j,\ell}(f_{j,\ell}) \right], \tag{1}$$

where the index ℓ goes over the set of neighboring communities of community j including community j itself.

We define g_i as the fraction of nodes in community i which belong to the GC. Accordingly, g_i is the probability that a randomly selected node in community i survived the attack and has at least one link which leads to the GC. Hence, g_i is obtained by the following equation:

$$g_i = p_i \left[1 - \prod_{j} G_{i,j}(f_{i,j}) \right], \tag{2}$$

where the index j goes over the set of neighboring communities of community i including community i itself.

Next, we obtain the MGC equations for a multiplex with two layers, A and B. Here, we define $f_{i,j}$ for each layer as the probability that a randomly selected link (that passes from community i to community j) does not lead to the MGC. Therefore, $1-f_{i,j}$ is the probability that the reached node survived the attack and has, in both layers, at least one neighbor that belongs to the MGC. In principle, the degree distributions of the layers can be different, and hence the functions of the components $f_{i,j}$, $G_{i,j}$, and $H_{i,j}$ should be different. From here, we distinguish the two layers by adding indexes A and B. Suppose that the survival probability for each community j after the initial attack is p_j, thus $f^A_{i,j}$ fulfill the equations

$$1-f^A_{i,j}=p_j\left[1-H^A_{j,i}\left(f^A_{j,i}\right)\prod_{\ell\neq i}G^A_{j,\ell}\left(f^A_{j,\ell}\right)\right]\times\left[1-\prod_{\ell}G^B_{j,\ell}\left(f^B_{j,\ell}\right)\right], \tag{3}$$

where the index ℓ goes over the set of neighboring communities of community j including community j itself. From symmetry, the equations for $1-f^B_{i,j}$ are the same but with switching between A and B. The MGC of community i, P_{∞_i}, is the probability that a randomly selected node in community i survived the initial attack and has in both layers at least one neighbor that belongs to the MGC. Thus,

$$P_{\infty i}=p_i\left[1-\prod_{j}G^A_{i,j}\left(f^A_{i,j}\right)\right]\left[1-\prod_{j}G^B_{i,j}\left(f^B_{i,j}\right)\right], \tag{4}$$

where the index j goes over the set of neighboring communities of community i including community i itself. The set of symmetric Eqs. (3) for $f^A_{i,j}$ and $f^B_{i,j}$ can be solved iteratively in such a way that each iteration represents a stage in the cascade of failures (see the Appendix, Sec. 1, for a more detailed discussion).

In the limit of infinitely large ER communities, it is acceptable to consider the ER degree distributions as Poisson. If all distributions $P_{i,j}(k)$ are Poisson, then $G_{i,j}(x)=H_{i,j}(x)=\exp[\langle k_{i,j}\rangle(x-1)]$ and all probabilities $f_{i,j}$ for the same community j but different i satisfy the same equation and hence they must be equal and we define $f_j\equiv f_{i,j}$. Thus, Eqs. (1) and (2) are significantly simplified and we obtain $f_j=(1-g_j)$. Hence, the probability that a node in community i belongs to the GC fulfills the following equation:

$$g_i=p_i\left[1-e^{-\sum_j\langle k_{i,j}\rangle g_j}\right]. \tag{5}$$

When the two layers of multiplex A and B follow Poisson distributions, and average degrees $\langle k_{i,j}\rangle_A$ and $\langle k_{i,j}\rangle_B$, respectively, Eq. (4) gives

$$P_{\infty i}=p_i\left[1-e^{-\sum_j\langle k_{i,j}\rangle_A P_{\infty j}}\right]\left[1-e^{-\sum_j\langle k_{i,j}\rangle_B P_{\infty j}}\right], \tag{6}$$

which is a generalization of the MGC equation for a single community of an ER multiplex, given in Eq. (40) of Ref. [3], to the case of many communities.

We next analyze the robustness of our community multiplex model with respect to localized attacks. To this end, we consider the case where all nodes within a radius r_h (radius hole), from the center of the multiplex, are removed from the network. When m is an even number, then the center of the multiplex is at the corner of four neighboring ER communities, or else it is in the center of one ER. Note that r_h translates into the value of p_i by counting the fraction of lattice sites outside the hole of radius r_h in the damaged communities.

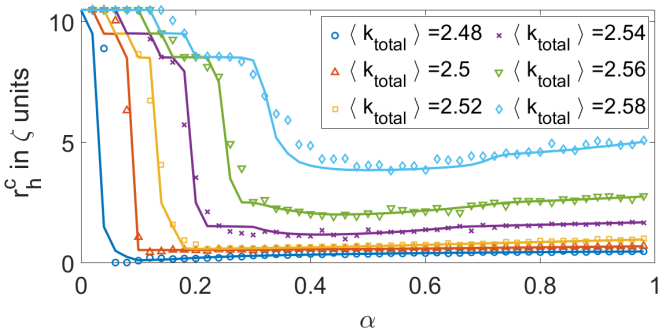

FIG. 2. The critical attack size r_h^c as a function of α for different $\langle k_{\text{total}}\rangle$ values. For every $\langle k_{\text{total}}\rangle$ the lines represent the theory of Eq. (6) and the symbols represent simulation results for finite lattices. For the simulations we set $L=2100$ and $\zeta=100$, with an average over five runs for each data point.

We find for networks with different system parameters, by simulations and theory, what is the critical radius r_h^c needed to cause a system collapse. We find the accurate value of r_h^c through a binary search, where increasing or decreasing of the radius attack is determined by the MGC size. At a given radius attack r_h, if the MGC size remains in order of the system size then we increase r_h, and otherwise—we decrease it. We define a threshold condition for the MGC size, below which we assume that the MGC is zero. For the numerical calculations of the theory we set the threshold to be 10^{-12}, and for the simulations (after some tests) a fraction of 0.1 of the system size seems to provide a good threshold condition. Each community consists of at least $\zeta^2=10^4$ nodes, so we can calculate numerically with good approximation the fraction of nodes that fail in each community for an attack r_h. In addition, since we study the case of a symmetrical two-dimensional square lattice, for the theoretical calculations [using Eq. (6)] we set $\langle k_{i,j}\rangle_A$ and $\langle k_{i,j}\rangle_B$ to be $\langle k_{\text{inter}}\rangle/4$ for $i\neq j$ and $\langle k_{\text{intra}}\rangle$ for $i=j$.

We find that for a network with structure parameters within a certain parameter range of L, ζ, and $\langle k_{\text{total}}\rangle$, there are two regimes that are divided by a critical α_c (see Fig. 2). For $\alpha>\alpha_c$ we have a metastable regime, where a finite-size localized attack larger than r_h^c causes cascading failures, leading to system collapse. In this regime, first, the critical radius r_h^c depends weakly on the interconnectivity parameter α. Second, r_h^c is independent of the number of communities (see Fig. 5 in the Appendix). Note that the metastable regime located in the narrow interval of $\langle k_{\text{total}}\rangle$ above $k_c\approx 2.4554$, where k_c is the critical average degree below which a single ER multiplex collapses without any initial damage [1]. In marked contrast, for $\alpha<\alpha_c$, the critical attack r_h^c is $\sim 0.5L$, i.e., removing the entire system. Therefore, a different α—for a fixed $\langle k_{\text{total}}\rangle$—can completely change the system's resilience to localized attacks. Remarkably, networks with the same $\langle k_{\text{total}}\rangle$ but larger interconnectivity ratio α can be more vulnerable to localized attacks than networks with small α where the communities are not well connected, but are more self-sufficient.

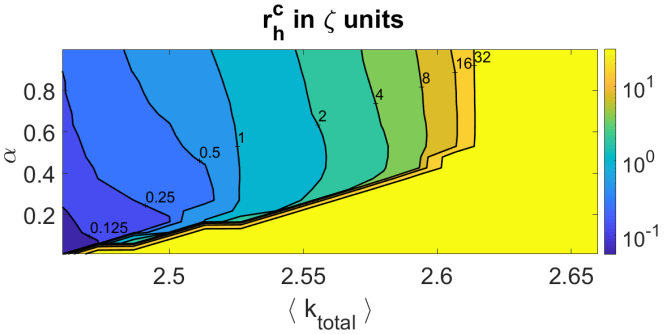

FIG. 3. Analytical results—Contour of the critical attack size r_h^c. Dependence of r_h^c on the average degree $\langle k_{\text{total}} \rangle$ and the interconnectivity parameter α, for $m = 100$. We sample with equal intervals 16 values for $\langle k_{\text{total}} \rangle$ and 20 values for α. The color bar on the right represents the size of r_h^c in ζ units (in log scale).

In addition, we obtain numerically based on Eq. (6) a phase diagram of r_h^c, for a large system with $m = 100$ in Fig. 3. The stable regime, where the system remains functional after any finite size of localized attack, is marked in yellow. Also, the phase diagram is the same for different m values, as shown in Fig. 5(c) in the Appendix, except for r_h^c that are of the order of the system size.

In order to understand how the damage (produced by the localized attack) spreads with time, we first produce the cascade of failures with $p_i = 1$. This configuration can be regarded as an initial state of the functional system. After this cascade stops we produce the localized attack of a given radius r_h^c. For example, for the simulations in Fig. 4, we perform the attack on step $time = 19$ after the system reaches equilibrium. After the attack, there is a long latent period during which only a few nodes fail at every time step, and they are located mostly in the vicinity of the attack area. Then, the damage quickly spreads until it reaches the edges of the system. The spreading process explains why the attack size does not depend on the system size.

IV. DISCUSSION

It is often attractive to build low-connectivity networks because they are typically less costly. This low connectivity, (i.e., relatively small $\langle k_{\text{total}} \rangle$ in our model) can cause susceptibility to various local failures for certain systems. Here we have investigated the stability of realistic interdependent networks, consisting of interconnected communities embedded in space, against local failures. We develop a theory for calculating the magnitude of the critical damage needed to destroy the entire system for different parameters of connectivity and spatiality. Our approach is similar to the finite-element method which is applied here to the network of communities, where each community is treated as an element, participating in a system of equations. We find that for the same $\langle k_{\text{total}} \rangle$ (and, hence, the same cost) the networks with low interconnectivity α are more robust against localized attacks than the systems in which the communities are well connected. If α is large, the damage produced by the localized attack spreads over the entire system. For small α, the damage does not spread. Thus, the interlinks connecting neighboring communities could serve as

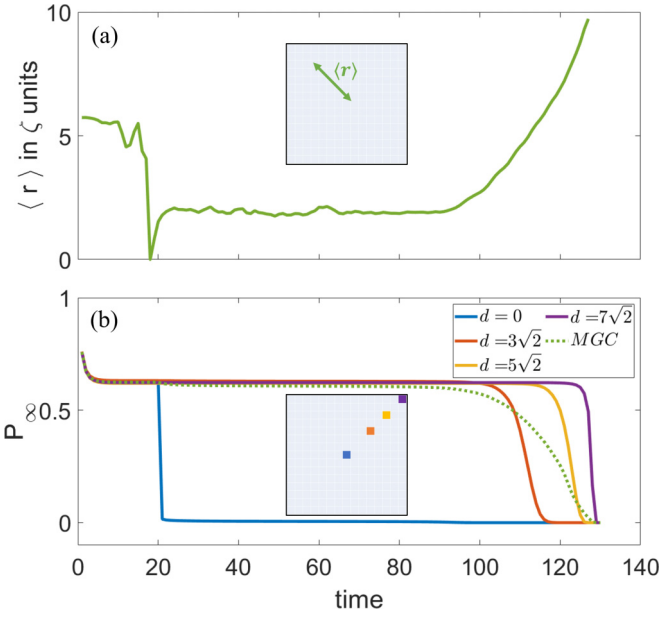

FIG. 4. The cascading failures near the critical point. Propagation of a local damage with a radius slightly above the critical size r_h^c. (a) The average distance from the center, $\langle r \rangle$, of the nodes that fail at every iteration. The inset figure is an illustration of the network. (b) The continuous lines represent the size of $P_{\infty j}$, for four communities having different distances d in ζ units from the center (where the critical hole was removed), as a function of time. The colors of the lines correspond to the colors of the painted communities in the inset figure. The dotted line shows the MGC size over the whole multiplex ($\sum_j P_{\infty j}$). For the simulations we set $L = 4500$, $\zeta = 300$, $\langle k_{\text{total}} \rangle = 2.5$, and $\alpha = 0.4$. The critical size r_h^c for this simulation, which was obtained through a binary search, is $r_h^c = 0.57$ in ζ units.

vehicles of damage propagation rather than for stabilizing the system. This finding explains why islanding, the strategy that the electrical engineers employed by dividing the system into almost isolated self-sustained islands, is an efficient strategy against cascading failures in the power grid.

In addition, we study the dynamical process of cascading and find a long latent period during which the number of failed nodes is very small and they are localized close to the initial attack. During this period, a relatively small intervention by reinforcing a few nodes can stop the propagation of the cascade of failures. After the latent period is over, the damage quickly spreads over the entire system and there is no economic way to stop it.

ACKNOWLEDGMENTS

We thank the Italian Ministry of Foreign Affairs and International Cooperation jointly with the Israeli Ministry of Science, Technology, and Space (MOST); the Israel Science Foundation; the BIU Center for Research in Applied Cryptography and Cyber Security; the Binational Israel-China Science Foundation (Grant No. 3132/19); NSF-BSF (Grant No. 2019740); and DTRA (Grant No. HDTRA-1-19-10016) for financial support. D.V. thanks the PBC of the Council for Higher Education of Israel for the Fellowship Grant and H. Sanhedrai for valuable discussions.

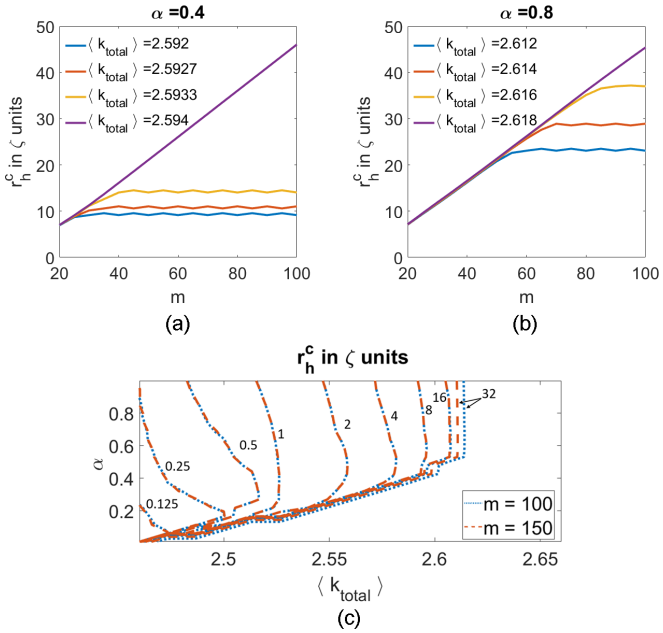

FIG. 5. The dependence of the critical attack size r_h^c on the number of communities. The number of communities is $m \times m$; therefore the dependence on m expresses the dependence of r_h^c on the number of communities. In panels (a) and (b) we show two behaviors of r_h^c for $\alpha = 0.4$ and $\alpha = 0.8$. For values of $\langle k_{\text{total}} \rangle$ near criticality, r_h^c initially grows with m and then, from a certain m, reaches a stable value. This stable value oscillates between two values of r_h^c which correspond to even and odd values of m. For large $\langle k_{\text{total}} \rangle$ values, r_h^c grows linearly with m and is approximately $0.5L$. In panel (c) we show the same contour lines of r_h^c as in Fig. 3 in the main text, with the original case of $m = 100$ and the additional case of $m = 150$. We see that both m values give identical results except near the border where $r_h^c \sim 0.5L$ (in the last contour line).

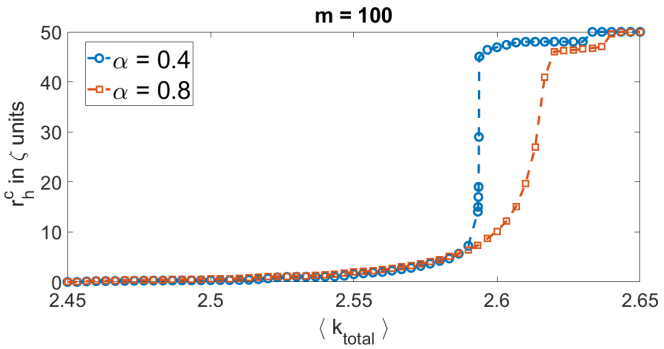

FIG. 6. The dependence of the critical attack size r_h^c on the total degree. Here we show (for $m = 100$) that r_h^c increases with $\langle k_{\text{total}} \rangle$, when for $\alpha = 0.4$ the transition is sharper than for $\alpha = 0.8$. This result explains why the jump in Fig. 5(a) is larger than that in Fig. 5(b).

APPENDIX

1. The cascading failures for a multiplex with two layers

In this section, we calculate the MGC size by analyzing the cascading failures along with applying the GC formulas for each layer separately [Eqs. (1) and (2) in the main text]. If we introduce vectors $\vec{f}$ with components $f_{i,j}$, $\vec{p}$ with components p_i, and $\vec{g}$ with components g_i, then Eq. (1) in the main text can be written in a symbolic vector form:

$$\vec{f} = \vec{\Phi}(\vec{f}, \vec{p}). \tag{A1}$$

This equation can be solved by the iteration method starting with $\vec{f} = 0$, and it will uniquely define vector $\vec{f}(\vec{p})$ as the function of vector $\vec{p}$. Analogously, Eq. (2) in the main text can be presented in a vector form:

$$\vec{g} = \vec{\Psi}(\vec{f}, \vec{p}). \tag{A2}$$

For generality, we assume that in this equation the vectors $\vec{f}$ and $\vec{p}$ are two arbitrary vectors, independent of one another.

Now we obtain equations for the MGC of the multiplex. Suppose that the survival probability vector after the initial attack is $\vec{p}(0)$ and that the vector of survival probabilities after stage t of the cascade is $\vec{p}(t)$. In principle, for the layers of the multiplex, A and B, the degree distributions can be different, and hence the functions $\vec{\Phi}$ and $\vec{\Psi}$ and the vectors $\vec{f}$ and $\vec{g}$ should be different. Therefore, we distinguish them by adding indexes A and B. Using the same logic as in Ref. [1], the equations of the cascade of failures starting from $t = 0$ are as follows:

$$\begin{aligned}
\vec{f}_A(2t) &= \vec{\Phi}_A[\vec{f}_A(2t), \vec{p}(2t)], \\
\vec{g}_A(2t) &= \vec{\Psi}_A[\vec{f}_A(2t), \vec{p}(2t)], \\
\vec{p}(2t+1) &= \vec{\Psi}_A[\vec{f}_A(2t), \vec{p}(0)], \\
\vec{f}_B(2t+1) &= \vec{\Phi}_B[\vec{f}_B(2t+1), \vec{p}(2t+1)], \\
\vec{g}_B(2t+1) &= \vec{\Psi}_B[\vec{f}_B(2t+1), \vec{p}(2t+1)], \\
\vec{p}(2t+2) &= \vec{\Psi}_B[\vec{f}_B(2t+1), \vec{p}(0)],
\end{aligned} \tag{A3}$$

where $\vec{g}_A(t)$ and $\vec{g}_B(t)$ are the fraction of nodes of each community in the giant component at stage t, and $\vec{p}(t)$ is the effective fraction of survived nodes representing stage t of the cascade of failures as a percolation process after a random attack. As $t \to \infty$ the vectors $\vec{g}_A(t)$ and $\vec{g}_B(t)$ will converge to the mutual giant component $\vec{P}_\infty$.

2. Analytical results of critical attack size r_h^c as a function of the system parameters

Figures 5 and 6 present the analytical results of the critical attack size r_h^c as a function of the system parameters.

[1] S. V. Buldyrev *et al.*, Catastrophic cascade of failures in interdependent networks, Nature (London) **464**, 1025 (2010).

[2] R. Parshani, S. V. Buldyrev, and S. Havlin, Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition, Phys. Rev. Lett. **105**, 048701 (2010).

[3] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, Robustness of a network formed by n interdependent networks with a

one-to-one correspondence of dependent nodes, Phys. Rev. E **85**, 066134 (2012).
[4] G. J. Baxter, S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Avalanche Collapse of Interdependent Networks, Phys. Rev. Lett. **109**, 248701 (2012).
[5] M. De Domenico, A. Solé-Ribalta, E. Cozzo, M. Kivelä, Y. Moreno, M. A. Porter, S. Gómez, and A. Arenas, Mathematical Formulation of Multilayer Networks, Phys. Rev. X **3**, 041022 (2013).
[6] S.-W. Son *et al.*, Percolation theory on interdependent networks based on epidemic spreading, Europhys. Lett. **97**, 16006 (2012).
[7] M. Kivelä *et al.*, Multilayer networks, J. Complex Networks **2**, 203 (2014).
[8] S. Boccaletti *et al.*, The structure and dynamics of multilayer networks, Phys. Rep. **544**, 1 (2014).
[9] F. Radicchi, Percolation in real interdependent networks, Nat. Phys. **11**, 597 (2015).
[10] M. M. Danziger, I. Bonamassa, S. Boccaletti, and S. Havlin, Dynamic interdependence and competition in multilayer networks, Nat. Phys. **15**, 178 (2019).
[11] G. Bianconi, *Multilayer Networks* (Oxford University, Oxford, 2018).
[12] G. Bianconi, Statistical mechanics of multiplex networks: Entropy and overlap, Phys. Rev. E **87**, 062806 (2013).
[13] D. Cellai, E. Lopez, J. Zhou, J. P. Gleeson, and G. Bianconi, Percolation in multiplex networks with overlap, Phys. Rev. E **88**, 052811 (2013).
[14] G. Bianconi and F. Radicchi, Percolation in real multiplex networks, Phys. Rev. E **94**, 060301(R) (2016).
[15] F. Coghi, F. Radicchi, and G. Bianconi, Controlling the uncertain response of real multiplex networks to random damage, Phys. Rev. E **98**, 062317 (2018).
[16] M. Barthélémy, Spatial networks, Phys. Rep. **499**, 1 (2011).
[17] 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).
[18] 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).
[19] S. Shao *et al.*, Percolation of localized attack on complex networks, New J. Phys. **17**, 023049 (2015).
[20] D. Vaknin, M. M. Danziger, and S. Havlin, Spreading of localized attacks in spatial multiplex networks, New J. Phys. **19**, 073037 (2017).
[21] S. Fortunato, Community detection in graphs, Phys. Rep. **486**, 75 (2010).
[22] E. Bullmore and O. Sporns, The economy of brain network organization, Nat. Rev. Neurosci. **13**, 336 (2012).
[23] A. Halu *et al.*, The multiplex network of human diseases, npj Syst. Biol. Appl. **5**, 1 (2019).
[24] K. A. Eriksen, I. Simonsen, S. Maslov, and K. Sneppen, Modularity and Extreme Edges of the Internet, Phys. Rev. Lett. **90**, 148701 (2003).
[25] R. Guimera *et al.*, The worldwide air transportation network: Anomalous centrality, community structure, and cities global roles, Proc. Natl. Acad. Sci. USA **102**, 7794 (2005).
[26] J. P. Bagrow, S. Lehmann, and Y.-Y. Ahn, Robustness and modular structure in networks, Network Sci. **3**, 509 (2015).
[27] L. M. Shekhtman, S. Shai, and S. Havlin, Resilience of networks formed of interdependent modular networks, New J. Phys. **17**, 123007 (2015).
[28] G. Dong *et al.*, Resilience of networks with community structure behaves as if under an external field, Proc. Natl. Acad. Sci. U.S.A. **115**, 6911 (2018).
[29] B. Gross, H. Sanhedrai, L. Shekhtman, and S. Havlin, Interconnections between networks acting like an external field in a first-order percolation transition, Phys. Rev. E **101**, 022316 (2020).
[30] A. Bunde and S. Havlin, *Fractals and Disordered Systems* (Springer-Verlag, New York, 1991).
[31] D. Stauffer and A. Aharony, *Introduction to Percolation Theory* (Taylor & Francis, London, 1994).
[32] R. Cohen and S. Havlin, *Complex Networks: Structure, Robustness and Function* (Cambridge University, Cambridge, England, 2010).
[33] M. Newman, *Networks: An Introduction* (Oxford University, Oxford, 2010).
[34] S. Rinaldi, J. Peerenboom, and T. Kelly, Identifying, understanding, and analyzing critical infrastructure interdependencies, IEEE Control Systems **21**, 11 (2001).
[35] P. Hines *et al.*, The topological and electrical structure of power grids, in *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences* (IEEE Computer Society, USA, 2010), pp. 1–10.
[36] M. J. O. Pocock, D. M. Evans, and J. Memmott, The robustness and restoration of a network of ecological networks, Science **335**, 973 (2012).
[37] D. Y. Kenett and S. Havlin, Network science: A useful tool in economics and finance, Mind & Soc. **14**, 155 (2015).
[38] M. A. Di Muro, S. V. Buldyrev, H. E. Stanley, and L. A. Braunstein, Cascading failures in interdependent networks with finite functional components, Phys. Rev. E **94**, 042304 (2016).
[39] B. Gross *et al.*, Multi-universality and localized attacks in spatially embedded networks, in *Proceedings of the Asia-Pacific Econophysics Conference 2016—Big Data Analysis and Modeling toward Super Smart Society—(APEC-SSS2016)* [JPS Conf. Proc. 16, 011002 (2017)].
[40] I. Bonamassa, B. Gross, M. M. Danziger, and S. Havlin, Critical Stretching of Mean-Field Regimes in Spatial Networks, Phys. Rev. Lett. **123**, 088301 (2019).
[41] M. M. Danziger *et al.*, The effect of spatiality on multiplex networks, Europhys. Lett. **115**, 36002 (2016).
[42] S. Brenner and R. Scott, *The Mathematical Theory of Finite Element Methods*, Texts in Applied Mathematics Vol. 15 (Springer Science & Business Media, Berlin, 2007).
[43] M. E. J. Newman, The structure and function of complex networks, SIAM Rev. **45**, 167 (2003).