Geometric Correlations Mitigate the Extreme Vulnerability of Multiplex Networks against Targeted Attacks

Kaj-Kolja Kleineberg,[1,*] Lubos Buzna,[2] Fragkiskos Papadopoulos,[3] Marián Boguñá,[4,5] and M. Ángeles Serrano[4,5,6]
[1]Computational Social Science, ETH Zurich, Clausiusstrasse 50, CH-8092 Zurich, Switzerland
[2]University of Zilina, Univerzitna 8215/1, SK-01026 Zilina, Slovakia
[3]Department of Electrical Engineering, Computer Engineering and Informatics, Cyprus University of Technology, 33 Saripolou Street, 3036 Limassol, Cyprus
[4]Departament de Física de la Matèria Condensada, Universitat de Barcelona, Martí i Franquès 1, E-08028 Barcelona, Spain
[5]Universitat de Barcelona Institute of Complex Systems (UBICS), Universitat de Barcelona, E-08028 Barcelona, Spain
[6]ICREA, Passeig Lluís Companys 23, E-08010 Barcelona, Spain
(Received 7 February 2017; revised manuscript received 30 March 2017; published 25 May 2017)

We show that real multiplex networks are unexpectedly robust against targeted attacks on high-degree nodes and that hidden interlayer geometric correlations predict this robustness. Without geometric correlations, multiplexes exhibit an abrupt breakdown of mutual connectivity, even with interlayer degree correlations. With geometric correlations, we instead observe a multistep cascading process leading into a continuous transition, which apparently becomes fully continuous in the thermodynamic limit. Our results are important for the design of efficient protection strategies and of robust interacting networks in many domains.

DOI: 10.1103/PhysRevLett.118.218301

Networks are ubiquitous in many domains of science and engineering, ranging from ecology to economics, and often form critical infrastructures, like the Internet and financial systems. Nowadays, these systems are increasingly interdependent [1] and form so-called multiplex or multilayer networks [2,3]. This interdependency implies that, if a node fails in one network layer, its counterparts in the other layers also fail simultaneously. This process can continue back and forth between the layers, which makes them especially vulnerable to failures. In particular, an abrupt transition can arise in mutual percolation when nodes are removed at random [3–5]. Interestingly, interlayer degree correlations [6–9] mitigate this vulnerability to random node removals, and the transition becomes continuous [10,11].

In real systems, failures may not always be random but, instead, the result of targeted attacks. Multiplexes are extremely vulnerable to them on high-degree nodes [12–14] and exhibit a discontinuous phase transition even in the presence of interlayer degree correlations [13]. Although it is highly important for many real systems, it is not well understood how this vulnerability can be mitigated. Previous results point to negative interlayer degree correlations as a mitigation factor [13], but real systems tend to show positive instead of negative interlayer degree correlations [6]. Are there other structural features that render multiplex networks robust against targeted attacks? And, most importantly, are these properties present in real multiplexes?

Here, we show that interlayer hidden geometric correlations [15] mitigate the vulnerability of multiplexes to targeted attacks. The removal of the highest-degree nodes triggers multiple cascades which do not destroy the system completely but eventually lead into a continuous percolation transition. Strikingly, we show that the strength of these geometric correlations in real systems is a good predictor of their robustness.

More specifically, we consider targeted attacks in two-layer multiplexes, where nodes are removed in decreasing order of their degrees among both layers. We rank all nodes i according to $K_i = \max(k_i^{(1)}, k_i^{(2)})$, where $k_i^{(j)}$ denotes the degree of node i in layer $j = 1, 2$. We remove nodes with higher K_i first (we undo ties at random) and reevaluate all K_i's after each removal. To measure the percolation state of the multiplex, we compute its mutually connected component (MCC) as the largest fraction of nodes that are connected by a path in every layer using only nodes in the component [4].

Figure 1 shows results for the real arXiv collaboration [16], *C. Elegans* [17], *Drosophila* [18], and *Sacc Pomb* [18] (see Table I, Supplemental Material [19], Sec. I, and Supplemental Videos I–IV) as well as for their reshuffled counterparts [an illustration of a targeted attack sequence is shown in Figs. 2(a)–2(d)]. To create the reshuffled counterpart, we randomly reshuffled the translayer node-to-node mappings by selecting one of the layers and randomly interchanging the internal IDs of the nodes in that layer. This process destroys all correlations between the layers without altering the layers' topologies (see Supplemental Material [19], Sec. I, for further details). We quantify the *vulnerability* of the real and reshuffled multiplexes by calculating the critical number of nodes, ΔN. The removal of this critical number reduces the size of the MCC from more than aM to less than M^β, where M is the initial size of the MCC before any nodes are removed, $a \leq 1$ is a threshold parameter, and $\beta < 1$ [26]. We set $a = 0.4$ and $\beta = 0.5$. The larger the ΔN, the more robust (less vulnerable) the system is. For the real arXiv multiplex we find that

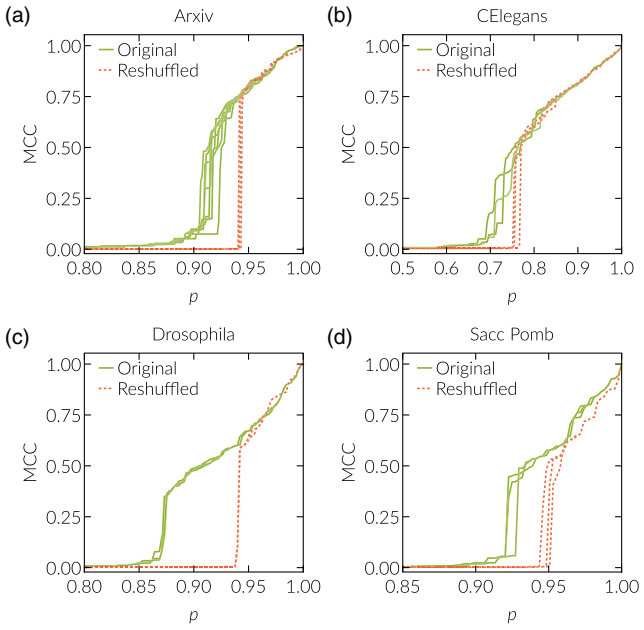

FIG. 1. (a) Relative size of the MCC against the fraction p of nodes remaining in the system for the arXiv (layers 1 and 2) collaboration multiplex (green lines) and for its reshuffled counterpart (red dashed lines). Different lines correspond to different realizations of the targeted attacks process. (b) shows the same for the *C. Elegans* multiplex (layers 2 and 3), (c) for *Drosophila* (layers 1 and 2), and (d) for *Sacc Pomb* (layers 3 and 4).

$\Delta N \approx 25$, while for its reshuffled counterpart $\Delta N_{\mathrm{rs}} = 1$. In fact, in the reshuffled system, the removal of a single node reduces the relative size of the MCC from 73% to only 0.25%. This is far more pronounced than the limits of $a = 40\%$ and $\sqrt{M}/M = 3.6\%$ and is enough to virtually disconnect this system. We have considered other layer pairs of the arXiv, as well as a large number of other real multiplexes from different domains (technological, social, and biological). We found that, in the vast majority of cases, the real system is significantly more robust against targeted attacks than its reshuffled counterpart (see Table I and Supplemental Material [19], Secs. I and II).

Below, we show that this increased robustness of real multiplexes to targeted attacks is due to hidden geometric correlations interwoven in their layers [15], which do not exist in their reshuffled counterparts. Specifically, each single network layer can be mapped (or embedded) into a separate hyperbolic space [27–29], where each node i is represented by its radial (popularity) and angular (similarity) coordinates r_i, θ_i, which are both significantly correlated in different layers, while hyperbolically closer nodes in each layer are connected with a higher probability (see Supplemental Material [19], Sec. I, for further details).

Radial correlations are equivalent to interlayer degree correlations [30]. Angular correlations, instead, lead to sets of nodes that are similar—close in the angular similarity space—in each layer of the multiplex [15]. The reshuffling process explained earlier destroys both radial and angular correlations between the layers. The extreme vulnerability of the reshuffled counterparts in comparison to the real systems raises fundamental questions: Are the radial (i.e., interlayer degree) correlations, or angular (i.e., geometric) correlations, or both, responsible for the robustness of real systems, and which of these correlations can help to avoid a catastrophic cascading failure when multiplexes are under targeted attack?

TABLE I. Analyzed data sets for selected layer pairs (see Supplemental Material [19], Sec. I, for all layer pairs). MCC denotes the initial size of the MCC, ΔN denotes the critical number of nodes whose removal reduces the MCC from 40% to $\sqrt{M}/M$ (in relative size), and ΔN_{rs} is the same for the reshuffled system. Values are averages over 100 realizations of the removal process. NMI denotes the normalized mutual information (see Supplemental Material [19], Sec. IX) and gives a measure of the strength of angular correlations between the layers of the considered real systems.

Data set	MCC	ΔN	ΔN_{rs}	NMI
arXiv layers 1, 2	790	25.2	1.0	0.58
Physician layers 1, 2	104	6.0	1.0	0.41
Internet layers 1, 2	4710	81.4	14.1	0.34
C. Elegans layers 2, 3	257	14.0	1.1	0.34
Sacc Pomb layers 3, 4	426	4.2	1.5	0.17
Drosophila layers 1, 2	449	8.4	2.0	0.26
Brain layers 1, 2	74	7.0	1.0	0.19
Rattus layers 1, 2	158	4.0	1.0	0.18
Air/train layers 1, 2	67	3.0	3.0	0.10

To investigate these questions, we use the geometric multiplex model (GMM) (see Supplemental Material [19], Sec. III) to generate synthetic two-layer multiplexes, which resemble the real equivalents. The model produces multiplexes with layers embedded into hyperbolic planes, whereby the strength of interlayer correlations between the radial and angular coordinates of nodes that simultaneously exist in both layers can be tuned by varying the model parameters $\nu \in [0, 1]$ and $g \in [0, 1]$. Radial correlations increase with parameter ν ($\nu = 0$ for no radial correlations, whereas $\nu = 1$ for maximal radial correlations). Similarly, angular correlations increase with parameter g ($g = 0$ for no angular correlations, while $g = 1$ for maximal angular correlations).

We find that synthetic multiplexes without angular correlations exhibit an extreme vulnerability to targeted attacks [see Fig. 2(e), Supplemental Material [19], Sec. III, and Supplemental Video V], similarly to the reshuffled counterparts of real systems (cf. Fig. 1 and Supplemental Material [19], Sec. II). In particular, if the multiplex is sufficiently large, then the removal of only a single node can reduce the size of the MCC from 40% to the square root of its initial size, thus destroying the connectivity of the system; see Fig. 2(f). The abrupt character of the transition is also reflected in the distribution of mutually connected component sizes. In the fragmented phase, the entire network is always split into very small components, even

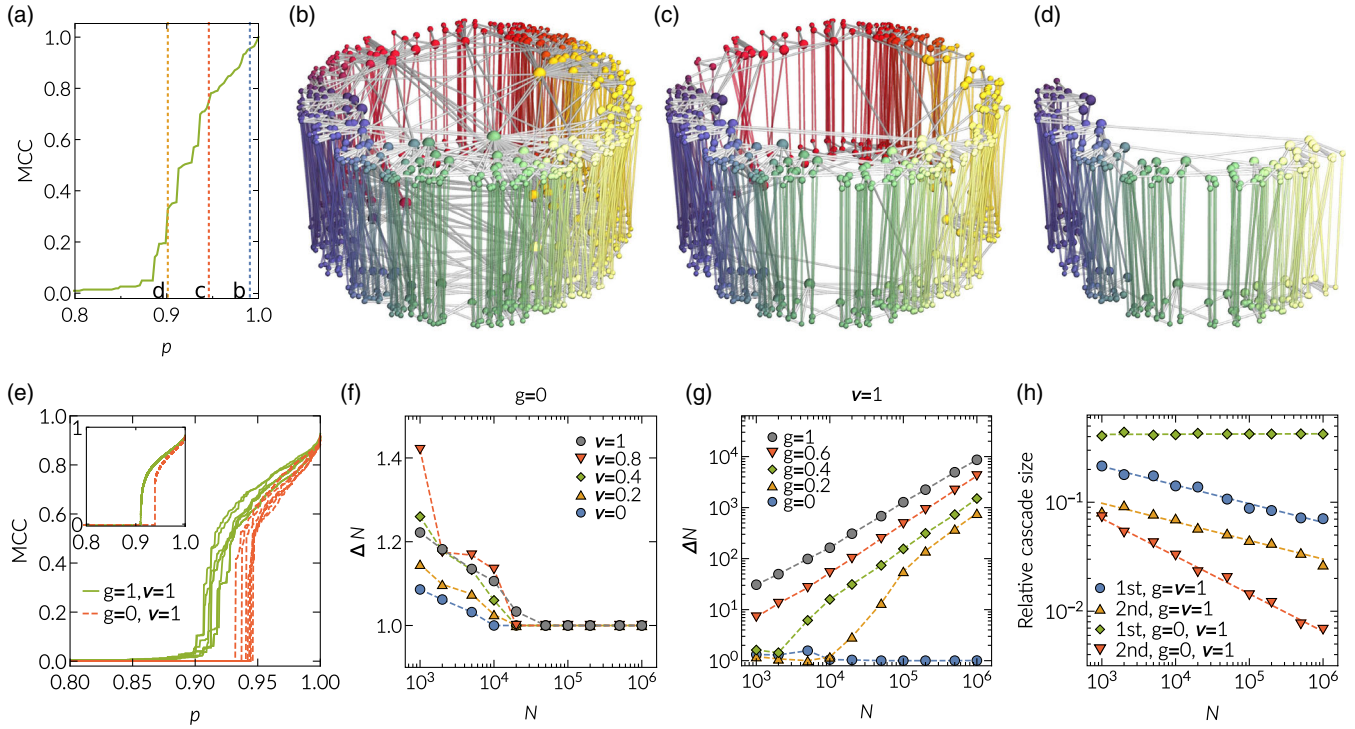

FIG. 2. Targeted attacks on synthetic multiplex networks generated by the GMM model (see the text). Each layer has a power law degree distribution with exponent $\gamma = 2.6$, average node degree $\langle k \rangle \approx 6$, and clustering $\bar{c} = 0.35$. (a)–(d) Here, each layer has $N = 500$ nodes, and we have set $g = 1$ and $\nu = 0$. (a) The relative size of the MCC as a function of the fraction of nodes remaining in the system p. (b) The MCC after the removal of four nodes [corresponding to the dashed blue line in (a)]. (c) The same as in (b) after the removal of 23 nodes [dashed red line in (a)]. (d) The MCC after the removal of 42 nodes [dashed yellow line in (a)]. (e) Evolution of the MCC in a two-layer synthetic multiplex with layers of size $N = 2 \times 10^3$ nodes. The inset shows the same for 10^6 nodes. (f) The critical number of nodes, ΔN, as a function of the system size N when there are no angular correlations, $g = 0$, and for different radial correlation strengths. The results are averages over 60 realizations (for $N < 10\,000$, we performed 1000 realizations). (g) The same as in (f) but for different values of the angular correlation strength g and for fixed $\nu = 1$. (h) shows the largest and second-largest cascade sizes (relative to the system size).

when the system is very close to the transition [see Fig. 3(a) and Supplemental Material [19], Sec. IV]. In the percolated phase, only nodes that do not belong to the MCC remain fragmented into small components [see Fig. 3(b) and Supplemental Material [19], Sec. IV]. This behavior is not affected by the strength of the radial (i.e., interlayer degree) correlations in the system. Thus, in contrast to the mitigation effect for random failures, interlayer degree correlations do not avoid an abrupt transition in the case of targeted attacks and essentially do not affect the robustness of the system.

On the other hand, this extreme vulnerability is mitigated if angular correlations are present. In Figs. 2(a)–2(e), we show the MCC percolation transition for maximal angular correlations (see also Supplemental Material [19], Secs. II and III, and Supplemental Video V). We observe that the transition does indeed start with a multistep cascading process for relatively small system sizes. However, as shown in Figs. 2(f) and 2(g), the critical number of nodes, ΔN, scales with the system size in the presence of angular correlations (see also Supplemental Material [19], Sec. V), while it always converges to one for large system sizes if angular correlations are absent. Moreover, as shown in Fig. 2(h), the relative size of the largest jump after a single node removal decreases with the system size, in stark contrast to the case without angular correlations, where this quantity becomes size independent. This suggests that, in the thermodynamic limit, the system undergoes a continuous transition [see the inset in Fig. 2(e)]. Furthermore, the size of the second-largest component scales with the system size like N^{σ}, with $\sigma \approx 0.84$ [see Figs. 3(d) and 3(e) and Supplemental Material [19], Sec. VI]. Finally, at the transition, the distribution of component sizes follows a power law [see Fig. 3(c) and Supplemental Material [19], Sec. IV]. Thus, we conjecture that angular correlations can lead to a multistep cascading process for relatively small system sizes and can give rise to a continuous transition in the thermodynamic limit (happening in a range of parameters of the model—including those used in Fig. 2—such that the multiplex layers have a strong metric structure but do not lose the small-world property in the targeted attack process; see Supplemental Material [19], Sec. VII). This behavior is not affected by the strength of radial (i.e., interlayer degree) correlations and cannot be explained by the link overlap induced by geometric correlations (see Supplemental Material [19], Sec. VIII). Taken together, our results suggest that angular (similarity) correlations can mitigate the extreme vulnerability of real multiplexes against targeted attacks.

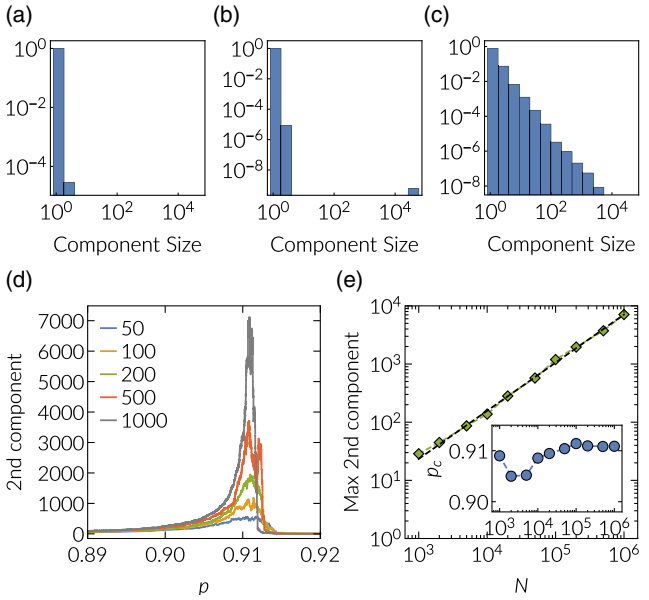

FIG. 3. (a)–(c) show the distribution of component sizes (probability density function) during the evolution of the MCC for two-layer synthetic multiplexes constructed with the GMM model. Each layer has a power law degree distribution with exponent $\gamma = 2.6$, average node degree $\langle k \rangle = 6$, and clustering $\bar{c} = 0.35$. In (a)–(c), each layer has $N = 5 \times 10^4$ nodes. The distribution of component sizes (a) directly before the transition ($p = 0.945\,39$) and (b) directly after ($p = 0.945\,40$), when there are no radial or angular correlations, $\nu = 0$, and $g = 0$. (c) The distribution of component sizes at $p = 0.9078$ when there are maximal angular correlations, $g = 1$, and no radial correlations, $\nu = 0$. (d) The absolute size of the second-largest MCC as a function of p for different layer sizes N as indicated in the legend ($\times 10^3$); for each size, the results are averages over 60 realizations of the multiplex [as in (e)]. (e) The scaling of the maximum of the second-largest MCC. The black dashed line shows a fit $\propto N^{0.84}$, while the inset shows the value of $p = p_c$ where the maximum is realized.

We can validate this conclusion in real systems. To this end, we compare the vulnerability of each of the considered real multiplexes (see Table I and Supplemental Material [19], Sec. I) with that of its reshuffled counterpart. We define the relative mitigation of vulnerability as

$$\Omega = \frac{\Delta N - \Delta N_{\mathrm{rs}}}{\Delta N + \Delta N_{\mathrm{rs}}}, \tag{1}$$

where ΔN and ΔN_{rs} are the number of nodes needed for the critical reduction of the size of the MCC of the real and reshuffled systems, respectively; see Table I and Supplemental Material [19], Sec. I. Ω is a measure of how much more resilient the real networks are compared to their reshuffled counterparts. Next, we study how Ω behaves as a function of the strength of angular correlations in the considered real systems. We quantify the strength of interlayer angular correlations by calculating the normalized mutual information (NMI) between the inferred angular coordinates of nodes in different layers (see Supplemental Material [19], Sec. IX). A larger NMI means higher angular correlations. We find a strong positive correlation ($\rho \approx 0.6$) between the strength of angular correlations in the real systems and their relative mitigation of vulnerability; see Fig. 4. This finding validates our previous arguments with real data and highlights the importance of angular correlations in making real multiplexes robust against targeted attacks.

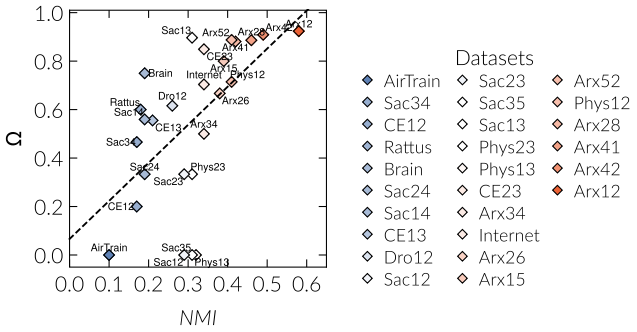

FIG. 4. Relative mitigation of vulnerability Ω [Eq. (1)] as a function of the NMI, which is a measure of the strength of angular correlations between the layers of the considered real systems (see Supplemental Material [19], Sec. IX, for details).

The gain of robustness due to angular correlations can be understood intuitively by the formation of macroscopic mutually connected structures on the periphery of the hyperbolic disk in each layer. After enough nodes are removed, the remaining multiplex resembles a "double ring" [Fig. 2(c)], because the higher-degree nodes which have been removed had lower radial coordinates and hence were closer to the center of the disk. If angular correlations are present, the remaining lower-degree nodes that are close in one layer tend to also be close in the other layer. As a consequence, the double ring contains macroscopic mutually connected structures [Fig. 2(d)] that sustain connectivity in the system. Notice that the mitigation of the extreme vulnerability of multiplexes by the effect of angular correlations is directly related to their geometric nature and cannot be explained by any topological feature. To support this point, we checked whether interlayer clustering correlations (clustering being the topological feature which is more directly related to the metric properties of networks [31]) or edge overlap induced by geometric correlations are sufficient to produce the mitigation effect. The results (see Supplemental Material [19], Secs. VIII and X) indicate that, in the absence of angular correlations, neither clustering correlations nor overlap can explain the observed mitigation effect. We take this to be a new validation of the geometric nature of complex networks and of the role of geometric correlations in multiplexes.

In conclusion, we have shown that the strength of geometric (similarity) correlations in real multiplex networks is a good predictor for their robustness against targeted attacks, providing, for the first time, strong empirical evidence for the relevance of this mechanism in real systems. Using a geometric multiplex network model, we have shown that

multiplex networks are extremely vulnerable against targeted attacks, exhibiting a discontinuous phase transition if geometric (similarity) correlations are absent. Contrarily, the presence of such correlations mitigates this vulnerability significantly, inducing a multistep cascading process in relatively small systems which does not destroy the system completely but leads into an eventually smooth percolation transition, with results suggesting that it can be fully continuous in the thermodynamic limit. In particular, the critical number of nodes that have to be removed to disconnect the system scales with the system size only if geometric correlations are present. Our results can help when designing efficient protection strategies and more robust and controllable interdependent systems. In addition, the results highlight that dependent networks without similarity correlations are extremely vulnerable to targeted attacks. Finally, our findings pave the way for an exact analysis of the percolation properties of such systems via their hidden geometric spaces.

K-K. K. acknowledges support by the ERC Grant "Momentum" (324247); L. B. has been supported by Projects No. VEGA 1/0463/16 and No. APVV-15-0179 and FP 7 project ERAdiate (621386); F. P. acknowledges support by the EU H2020 NOTRE project (Grant No. 692058). M. A. S. and M. B. acknowledge support from a James S. McDonnell Foundation Scholar Award in Complex Systems, MINECO Projects No. FIS2013-47282-C2-1-P and No. FIS2016-76830-C2-2-P (AEI/FEDER, UE), and the Generalitat de Catalunya Grant No. 2014SGR608. M. B. acknowledges support from the ICREA Academia prize, funded by the Generalitat de Catalunya.

*kkleineberg@ethz.ch

[1] D. Helbing, Globally networked risks and how to respond, Nature (London) **497**, 51 (2013).
[2] M. Kivelä, A. Arenas, M. Barthelemy, J. P. Gleeson, Y. Moreno, and M. A. Porter, Multilayer networks, J. Complex Netw. **2**, 203 (2014).
[3] G. Bianconi, Multilayer networks: Dangerous liaisons? Nat. Phys. **10**, 712 (2014).
[4] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature (London) **464**, 1025 (2010).
[5] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, Networks formed from interdependent networks, Nat. Phys. **8**, 40 (2011).
[6] V. Nicosia and V. Latora, Measuring and modeling correlations in multiplex networks, Phys. Rev. E **92**, 032805 (2015).
[7] B. Min, S. D. Yi, K.-M. Lee, and K.-I. Goh, Network robustness of multiplex networks with interlayer degree correlations, Phys. Rev. E **89**, 042811 (2014).
[8] J. Y. Kim and K.-I. Goh, Coevolution and Correlated Multiplexity in Multiplex Networks, Phys. Rev. Lett. **111**, 058702 (2013).
[9] V. Gemmetto and D. Garlaschelli, Multiplexity versus correlation: The role of local constraints in real multiplexes, Sci. Rep. **5**, 9120 (2015).
[10] S. D. S. Reis, Y. Hu, A. Babino, J. S. Andrade, Jr., S. Canals, M. Sigman, and H. A. Makse, Avoiding catastrophic failure in correlated networks of networks, Nat. Phys. **10**, 762 (2014).
[11] M. Ángeles Serrano, Ľ. Buzna, and M. Boguñá, Escaping the avalanche collapse in self-similar multiplexes, New J. Phys. **17**, 053033 (2015).
[12] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin, Robustness of network of networks under targeted attack, Phys. Rev. E **87**, 052804 (2013).
[13] B. Min, S. D. Yi, K.-M. Lee, and K.-I. Goh, Network robustness of multiplex networks with interlayer degree correlations, Phys. Rev. E **89**, 042811 (2014).
[14] D.-w. Zhao, L.-h. Wang, Y.-f. Zhi, J. Zhang, and Z. Wang, The robustness of multiplex networks under layer node-based attack, Sci. Rep. **6**, 24304 (2016).
[15] K.-K. Kleineberg, M. Boguñá, M. Á. Serrano, and F. Papadopoulos, Hidden geometric correlations in real multiplex networks, Nat. Phys. **12**, 1076 (2016).
[16] M. D. Domenico, A. Lancichinetti, A. Arenas, and M. Rosvall, Identifying Modular Flows on Multilayer Networks Reveals Highly Overlapping Organization in Interconnected Systems, Phys. Rev. X **5**, 011027 (2015).
[17] M. D. Domenico, M. A. Porter, and A. Arenas, Muxviz: A tool for multilayer analysis and visualization of networks, J. Complex Netw. **3**, 159 (2015).
[18] M. D. Domenico, V. Nicosia, A. Arenas, and V. Latora, Structural reducibility of multilayer networks, Nat. Commun. **6**, 6864 (2015).
[19] See also Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.118.218301 for details on the datasets, which includes Refs. [20–25].
[20] F. Papadopoulos, M. Kitsak, M. Serrano, M. Boguñá, and D. Krioukov, Popularity versus similarity in growing networks, Nature (London) **489**, 537 (2012).
[21] D. Stauffer and A. Aharony, *Introduction to Percolation Theory* (Oxford University Press, New York, 1971).
[22] H. E. Stanley, *Introduction to Phase Transitions and Critical Phenomena* (Oxford University Press, New York, 1987).
[23] D. Sornette, *Critical Phenomena in Natural Sciences (Chaos, Fractals, Selforganization and Disorder: Concepts and Tools)*, Springer Series in Synergetics (Springer, New York, 2006).
[24] A. Kraskov, H. Stögbauer, and P. Grassberger, Estimating mutual information, Phys. Rev. E **69**, 066138 (2004).
[25] T. W. Anderson, *An Introduction to Multivariate Statistical Analysis*, Wiley Series in Probability and Mathematical Statistics (Wiley, New York, 1984).
[26] D. Achlioptas, R. M. D'Souza, and J. Spencer, Explosive percolation in random networks, Science **323**, 1453 (2009).
[27] M. Boguñá, F. Papadopoulos, and D. Krioukov, Sustaining the Internet with hyperbolic mapping, Nat. Commun. **1**, 62 (2010).

[28] F. Papadopoulos, C. Psomas, and D. Krioukov, Network mapping by replaying hyperbolic growth, IEEE/ACM Trans. Netw. **23**, 198 (2015).

[29] F. Papadopoulos, R. Aldecoa, and D. Krioukov, Network geometry inference using common neighbors, Phys. Rev. E **92**, 022807 (2015).

[30] D. Krioukov, F. Papadopoulos, M. Kitsak, A. Vahdat, and M. Boguñá, Hyperbolic geometry of complex networks, Phys. Rev. E **82**, 036106 (2010).

[31] M. A. Serrano, D. Krioukov, and M. Boguñá, Self-Similarity of Complex Networks and Hidden Metric Spaces, Phys. Rev. Lett. **100**, 078701 (2008).