Eur. Phys. J. Special Topics **223**, 2087–2106 (2014)

DOI: 10.1140/epjst/e2014-02251-6

THE EUROPEAN PHYSICAL JOURNAL SPECIAL TOPICS

Review

Vulnerability of network of networks

S. Havlin[1,a], D.Y. Kenett[2,b], A. Bashan[3,c], J. Gao[4,5,d], and H.E. Stanley[2,e]

[1] Department of Physics, Bar-Ilan University, Ramat Gan, Israel
[2] Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA
[3] Channing Division of Network Medicine, Brigham and Women's Hospital, and Harvard Medical School, Boston, MA 02115, USA
[4] Department of Automation, Shanghai Jiao Tong, University, 800 Dongchuan Road, Shanghai 200240, P.R. China
[5] Center for Complex Network Research and Department of Physics, Northeastern University, Boston, MA 02115, USA

Received 13 April 2014 / Received in final form 18 August 2014
Published online 24 October 2014

Abstract. Our dependence on networks – be they infrastructure, economic, social or others – leaves us prone to crises caused by the vulnerabilities of these networks. There is a great need to develop new methods to protect infrastructure networks and prevent cascade of failures (especially in cases of coupled networks). Terrorist attacks on transportation networks have traumatized modern societies. With a single blast, it has become possible to paralyze airline traffic, electric power supply, ground transportation or Internet communication. How, and at which cost can one restructure the network such that it will become more robust against malicious attacks? The gradual increase in attacks on the networks society depends on – Internet, mobile phone, transportation, air travel, banking, etc. – emphasize the need to develop new strategies to protect and defend these crucial networks of communication and infrastructure networks. One example is the threat of liquid explosives a few years ago, which completely shut down air travel for days, and has created extreme changes in regulations. Such threats and dangers warrant the need for new tools and strategies to defend critical infrastructure. In this paper we review recent advances in the theoretical understanding of the vulnerabilities of interdependent networks with and without spatial embedding, attack strategies and their affect on such networks of networks as well as recently developed strategies to optimize and repair failures caused by such attacks.

[a] e-mail: havlins@gmail.com
[b] e-mail: drorkenett@gmail.com
[c] e-mail: amir.bashan@channing.harvard.edu
[d] e-mail: jianxi.gao@gmail.com
[e] e-mail: hes@bu.edu

1 Introduction

The interdisciplinary field of network science has attracted great attention in recent years [1–27]. This has taken place because an enormous amount of data regarding social, economic, engineering, and biological systems has become available over the past two decades as a result of the information and communication revolution brought about by the rapid increase in computing power. The investigation and growing understanding of this extraordinary amount of data will enable us to make the infrastructures we use in everyday life more efficient and more robust. The original model of networks, random graph theory, developed in the 1960s by Erdős and Rényi (ER), is based on the assumption that every pair of nodes is randomly connected with the same probability (leading to a Poisson degree distribution). In parallel, lattice networks in which each node has the same number of links have been used in physics to model physical systems. While graph theory was a well-established tool in the mathematics and computer science literature, it could not adequately describe modern, real-world networks. Indeed, the pioneering observation by Barabási in 1999 [2], that many real networks do not follow the ER model but that organizational principles naturally arise in most systems, led to an overwhelming accumulation of supporting data, new models, and novel computational and analytical results, and led to the emergence of network science.

Significant advances in understanding the structure and function of networks, and mathematical models of networks have been achieved in recent years. These are now widely used to describe a broad range of complex systems, from techno-social systems to interactions amongst proteins. A large number of new measures and methods have been developed to characterize network properties, including measures of node clustering, network modularity, correlation between degrees of neighboring nodes, measures of node importance, and methods for the identification and extraction of community structures. These measures demonstrated that many real networks, and in particular biological networks, contain network motifs – small specific subnetworks– that occur repeatedly and provide information about functionality [8]. Dynamical processes, such as flow and electrical transport in heterogeneous networks, were shown to be significantly more efficient compared to ER networks [28,29].

Complex networks are usually non-homogeneous structures that exhibit a power-law form in their degree (number of links per node) distribution. These systems are called scale-free networks. Some examples of real-world scale-free networks include the Internet [3], the WWW [4], social networks representing the relations between individuals, infrastructure networks such as airlines [30,31], networks in biology, in particular networks of protein-protein interactions [32], gene regulation, and biochemical pathways, and networks in physics, such as polymer networks or the potential energy landscape network. The discovery of scale-free networks has led to a re-evaluation of the basic properties of networks, such as their robustness, which exhibit a character that differs drastically from that of ER networks. For example, while homogeneous ER networks are vulnerable to random failures, heterogeneous scale-free networks are extremely robust [4,5]. Much of our current knowledge of networks is based on ideas borrowed from statistical physics, e.g., percolation theory, fractal analysis, and scaling analysis. An important property of these infrastructures is their stability, and it is thus important that we understand and quantify their robustness in terms of node and link functionality. Percolation theory was introduced to study network stability and to predict the critical percolation threshold [5]. The robustness of a network is usually (i) characterized by the value of the critical threshold analyzed using percolation theory [33] or (ii) defined as the integrated size of the largest connected cluster during the entire attack process [34]. The percolation approach was also extremely useful in addressing other scenarios, such as efficient attacks or immunization [6,7,14,35,36],

for obtaining optimal path [37] as well as for designing robust networks [34]. Network concepts were also useful in the analysis and understanding of the spread of epidemics [38,39], and the organizational laws of social interactions, such as friendships [40,41] or scientific collaborations [42]. Moreira et al. investigated topologically-biased failure in scale-free networks and controlled the robustness or fragility by fine-tuning the topological bias during the failure process [43].

Because current methods deal almost exclusively with individual networks treated as isolated systems, many challenges remain [44]. In most real-world systems an individual network is one component within a much larger complex network of networks. As technology has advanced, coupling between networks has become increasingly strong. Node failures in one network will cause the failure of dependent nodes in other networks, and vice-versa [45]. This recursive process can lead to a cascade of failures throughout the network of networks system. The study of individual particles has enabled physicists to understand the properties of a gas, but in order to understand and describe a liquid or a solid the interactions between the particles are needed to be considered. Such is also the case in network theory, where the study of isolated single networks brings extremely limited results – real-world noninteracting systems are extremely rare in both classical physics and network study. Most real-world network systems continuously interact with other networks, especially since modern technology has accelerated network interdependency.

To adequately model most real-world systems, understanding the interdependence of networks and the effect of this interdependence on the structural and functional behavior of the coupled system is crucial. Introducing coupling between networks is analogous to the introduction of interactions between particles in statistical physics, which allowed physicists to understand the cooperative behavior of such rich phenomena as phase transitions. Surprisingly, recent results on mathematical models [45,46] show that analyzing complex systems as a network of coupled networks may alter the basic assumptions that network theory has relied on for single networks.

2 Cascading failures in interdependent networks

Complex systems, usually represented as complex networks, are rarely isolated but usually interdependent and interact with other systems [47–49]. The vulnerability of a single network is usually described by the percolation model in which the order parameter is the size of the giant connected component and the control parameter is the fraction of nodes not removed in the initial failure [50]. Recently it was shown that a coupled networks system is considerably more vulnerable than its isolated network components [45,46]. In interdependent networks nodes interactions are represented by two different types of links, connectivity and dependency links. Moreover, while single network disintegrate continuously as in a second order phase transition, a coupled network system disintegrate abruptly as in a first order phase transition. The requirement to be connected to the giant connected component, as in single-network-percolation, represents the need of a node (to function) to be connected to *the system*, but it does not matter through which path. In contrast, a dependency link represents the need of a node to get a critical supply in order to function from *one other specific node*. Without this supply it fails even if it is still connected to giant component. This type of models are based on the idea of mutual percolation in which the order parameter is the size of the mutual giant component [45,46,51–63]. The coupling between different networks induces a dynamical process of cascading failures. A failure of nodes in one network leads to a failure of dependent nodes in other networks, which in turn may cause further damage to the first network and so on. This cascading failures may totally fragment the entire system and the size of the

mutual giant component collapses to zero. It was shown that the coupling strength of the networks, represented by the fraction q of interdependent nodes, determines the way the system collapses [46,52,70]. For strong coupling, that is for high fraction of interdependent nodes, an initial damage can lead to cascading failures that yields an abrupt collapse of the system, in a form of a first-order phase transition. Reducing the coupling strength below a critical value, q_c, leads to a change from an abrupt collapse to a continuous decrease of the size of the network, in a form of a second-order phase transition. This new paradigm is in marked contrast to the common knowledge represented by a single network behavior. In any single network the percolation transition is always continuous, therefore, the damage due to a failure is a continuous function of the size of the damage. In sharp contrast, in interdependent networks, due to the cascading failures, the percolation transition may be discontinuous. In this case, a damage of even a single node can lead to failure of finite fraction of the whole system, which is clearly different from the continuous behavior in single networks. The existence of an abrupt collapse phenomena in interdependent networks makes such systems extremely risky. Thus, understanding this phenomena is critical for evaluating the systems' risks and vulnerability and for designing robust infrastructures [34].

Recently, four examples of network of networks (NON) that can be explicitly solved analytically have been introduced [52,70,71]: (i) a tree-like ER NON *fully* dependent, (ii) a tree-like random regular (RR) NON *fully* dependent, (iii) a loop-like ER NON *partially* dependent, and (iv) an RR network of *partially* dependent ER networks. All cases represent different generalizations of percolation theory for a single network. Next we discuss shortly the case of (i) and (iv).

2.1 Tree-like NON of ER networks

To study the robustness of a given network, one can apply percolation theory and ask what happens to the network after removing randomly a fraction of $1 - p$ of nodes. Removing the nodes, their edges become also non functional and thus are also removed. This may cause the breakdown of the network into clusters. When p is greater than a critical threshold p_c, there exists a giant component, P_∞, of the order of the initial network size, while for $p < p_c$ the network breaks down into small clusters. For ER network with average degree $\langle k \rangle$, P_∞ was derived analytically [64–67],

$$P_\infty = p[1 - e^{-\langle k \rangle P_\infty}]. \tag{1}$$

To study the robustness of interdependent networks systems, composed for example of two networks A and B, we begin by removing a fraction $1 - p$ of network A nodes and all the A-edges connected to these nodes. As an outcome, all the nodes in network B that are dependent on the removed A-nodes by A $\rightarrow$ B links are also removed since they depend on the removed nodes in network A. Their B edges are also removed. Further, the removed B nodes will cause the removal of additional nodes in network A which are connected to the removed B-nodes by B $\rightarrow$ A links. As a result, a cascade of failures that eliminates virtually all nodes in both networks can occur. As nodes and edges are removed, each network breaks up into connected components (clusters). The clusters in network A (connected by A-edges) and the clusters in network B (connected by B-edges) are different since the networks are each connected differently. If one assumes that small clusters (whose size is below certain threshold) become non-functional, this may invoke a recursive process of failures that we now formally describe. Our insights based on percolation theory is that when the network is fragmented the nodes belonging to the giant component connecting a

finite fraction of the network are still functional, but the nodes that are part of the remaining small clusters become non-functional. Thus, in interdependent networks only the giant mutually-connected cluster is of interest.

Gao et al. presented an exact expression for for tree-like NON of fully interdependent ($q = 1$, where q represents the degree of interdependency) ER networks, for the order parameter $P_\infty(p)$, the size of the mutual giant component for all p, k, and n values [52,70],

$$P_\infty = p[1 - e^{-\langle k\rangle P_\infty}]^n. \tag{2}$$

Here $1-p$ is the fraction of removed nodes in each network, $\langle k\rangle$ is the mean degree and n is the number of ER networks in the tree. The special case $n = 1$ is the known ER second-order percolation law for a single network [64–66]. In contrast, for any $n > 1$ the solution of (2) yields a first-order percolation transition, i.e., a discontinuity of P_∞ at p_c.

Gao et al. derived also p_c and $P_\infty(p_c)$ as a function of n for different $\langle k\rangle$ values,

$$p_c = [n\langle k\rangle(1 - f_c)^{(n-1)}]^{-1}, \tag{3}$$

$$P_\infty(p_c) = \frac{(1 - f_c)}{n\langle k\rangle f_c}, \tag{4}$$

and

$$f_c = -\left[nW\left(-\frac{1}{n}e^{-(1/n)}\right)\right]^{-1}, \tag{5}$$

where $W(x)$ represents the Lambert function [52].

Furthermore, when n is fixed and $\langle k\rangle$ is smaller than a critical number $k_{\min}(n)$, $p_c \geqslant 1$, which means that when $\langle k\rangle < k_{\min}(n)$ the NON will collapse even if a single node fails. The minimum average degree $k_{\min}$ as a function of the number of networks is

$$k_{\min}(n) = [nf_c(1 - f_c)^{(n-1)}]^{-1}. \tag{6}$$

Equations (2)–(6) are valid for all tree-like NON. Note that Eq. (6) yields the value of $k_{\min}(1) = 1$, reproducing the known ER result, that $\langle k\rangle = 1$ is the minimum average degree needed to have a giant component. For $n = 2$, Eq. (6) also yields results obtained in [45], i.e., $k_{\min} = 2.4554$. The abrupt first order transition in interdependent networks was shown recently to occur simultaneously with a second order percolation transition during the cascading failures [72].

2.2 NON of ER networks

Next we review results [70,71] for a NON in which each ER network is dependent on exactly m other ER networks. This system represents the case of RR network of ER networks. We assume that the initial attack on each network is $1 - p$, and each partially dependent pair of networks has the same fraction of dependency nodes q in both directions. The n equations for P_∞ can be solved analytically,

$$P_\infty = \frac{p}{2^m}(1 - e^{-\langle k\rangle P_\infty})[1 - q + \sqrt{(1 - q)^2 + 4qP_\infty}]^m. \tag{7}$$

It is found [71] that there is a critical coupling q_c is

$$q_c = \frac{\langle k\rangle + m - (m^2 + 2\langle k\rangle m)^{1/2}}{\langle k\rangle}. \tag{8}$$

For $q < q_c$ the percolation transition is continuous (second order) while for $q > q_c$ it is abrupt (first order). When the transition is second order ($q < q_c$), p_c is found to be,

$$p_c = \frac{1}{\langle k \rangle (1-q)^m}. \tag{9}$$

Furthermore, it is possible to calculate the critical point q_{max}, above which ($q > q_{max}$) the system is unstable and collapse even for $p = 1$

$$q_{max} = \frac{(a^{1/m} - 1)^2}{2(1 - 2z_c - z^{1/m})}, \tag{10}$$

where

$$a = \frac{1 - e^{\langle k \rangle (z_c - 1)}}{2^m (1 - z_c)}. \tag{11}$$

It is surprising that both the critical threshold and the giant component do not depend on the number of networks n, in contrast to tree-like NON, but only on the coupling q and on both degrees k and m. In the special case of $m = 0$, Eqs. (7) and (9) coincide with the known results for a single ER network. In summary, that when $q < q_c$ we have "weak coupling" represented by a second-order phase transition and when $q_c < q < q_{\max}$ we have "strong coupling" and a first-order phase transition. When $q > q_{\max}$ the system becomes unstable due to the "very strong coupling" between the networks, and a removal of a single node in one network may lead to the collapse of the NON. For the critical behavior of the tri-critical point q_c, see [46,73,74].

2.3 NON of scale free networks

We analyze here NetONets composed of SF networks with a power law degree distribution $P(k) \sim k^{-\lambda}$. The corresponding generating function is

$$G(z) = \frac{\sum_s^M [(k+1)^{1-\lambda} - k^{1-\lambda}] z^k}{(M+1)^{1-\lambda} - s^{1-\lambda}} \tag{12}$$

where s ($s = 2$ in this paper) is the minimal degree cutoff and M is the maximal degree cutoff.

SF networks approximate real networks such as the Internet, airline flight patterns, and patterns of scientific collaboration [2,4,20]. When SF networks are fully interdependent [45], $p_c > 0$, even in the case $\lambda \leqslant 3$ in contrast to a single network for which $p_c = 0$ [5]. We study the percolation of a RR network composed of interdependent SF networks by substituting their degree distribution and obtaining their generating functions. We assume, for simplicity, that all the networks in the NON have the same λ, s and M, and analyze the percolation of an RR NON of SF networks.

The generating function of the branching process is defined as $H(z) = G'(z)/G'(1)$, and it is used together with Eq. (12) to obtain the function $R(z)$ for RR of SF networks. Three regimes of coupling strength q are observed:

(i) When q is small ($q < q_c$), $R(z)$ is a monotonically increasing function of z, the system shows a second order phase transition, and the critical threshold p_c^{II} is obtained when $z \to 1$ which corresponds to $R(1) = \max\{R\} = \infty = 1/p_c^{II}$, i.e., $p_c^{II} = 0$.

(ii) When q is larger, $q_c < q < q_{\max}$, $R(z)$ as a function of z shows a peak which corresponds to a sharp jump to a lower value of P_∞ at z_c^I showing a first order phase transition. As z increases, $R(z)$ first decreases then increases with z and reach the maximal value of R at $z_c^{II} \to 1$ showing a second order phase transition. Furthermore, the threshold of first order phase transition is $p_c^I = 1/R(z_c^I)$, while for p below this sharp jump the system undergoes a smooth second order phase transition and the critical threshold is zero, similar to (i).

(iii) When q is above $q_{\max}$, $R(z)$ decreases with z first, and then increases with z, which corresponds to the system collapse.

Next we analyze the three regimes more rigorously.

(i) When q is small ($q < q_c$), $R(z)$ is a monotonically increasing function of z, the maximum of $R(z_c)$ is obtained when $z_c \to 1$, which corresponds to $P_\infty = 0$,

$$\max\{R\} = \lim_{z\to 1} \frac{H(z)-1}{z-1}(1-q)^m \doteq H'(1). \tag{13}$$

Thus, for $\lambda < 3$, the second order transition happens at $p_c^{II}(M) \to 0$, when $M \to \infty$, while for $\lambda > 3$ it remains finite for $M \to \infty$.

(ii) As q increases ($q \geqslant q_c$), $R(z)$ as a function of z shows a peak corresponding to $R(z) = R(z_c)$ for small values of z, $\mathrm{dR/dz} = 0$ (smaller root has the physical meaning), where $R = R_c = 1/p_c^I > 1$ which corresponds to the first order critical threshold where P_∞ as a function of p shows an abrupt jump. Furthermore, we define

$$P_\infty^- = \lim_{p\to p_c^I, p<p_c^I} P_\infty(p), \tag{14}$$

and

$$P_\infty^+ = \lim_{p\to p_c^I, p>p_c^I} P_\infty(p). \tag{15}$$

However the phase transition here is different from a normal first order phase transition where $P_\infty^- = 0$. In our interdependent networks system $P_\infty^- > 0$. After the sharp drop for $p < p_c^I$, P_∞ decreases smoothly to 0 and undergoes a second order phase transition. The critical threshold of the second order phase transition is described in (i). The specific case of two partially interdependent SF networks is studied also Zhou et al. [72].

(iii) As q increases further ($q > q_{max}$), $\frac{\mathrm{dR(z)}}{\mathrm{dz}}$ at $z = 0$ becomes negative, thus the NetONet will collapse even when a single node is initially removed. So the maximum values of q is obtained as

$$\frac{\mathrm{dR(z)}}{\mathrm{dz}}|_{z\to 0} = 0. \tag{16}$$

For the minimal degree cut-off $s = 2$, i.e. $P(0) = P(1) = 0$, when $q = q_{\max}$, $P_\infty(z)|_{z\to 0} = 1$ and $P'_\infty(z)|_{z\to 0} = -1$, so we get

$$q_{\max} = \frac{1}{m-1}. \tag{17}$$

Comparison between analytical and simulation results is shown in Fig. 1.

3 Vulnerability of interdependent spatially embedded networks

Current models focus on interdependent networks where space restrictions are not considered. Indeed, in some complex systems the spatial location of the nodes is not

relevant or not even defined, such as in proteins interaction networks [75–77] and the World Wide Web [5,78]. However, in many real-world systems, such as power grid networks, ad hoc communication networks and computer networks, nodes and links are located in Euclidian two-dimensional space [79]. Based on universality principles, the dimension of a network is a fundamental quantity to characterize its structure and basic physical properties [80,81]. Indeed, all percolation models whose links have a characteristic length, embedded in space of same dimension belong to *the same* universality class [80]. An example is power grid networks where the links have a characteristic length since their lengths follow an exponential distribution [81]. Due to universality considerations, any 2d network with links having a characteristics length scale, belong to the same universality class as regular lattices. Thus, to obtain the main features of an arbitrary system of interdependent networks embedded have been modeled in two dimensional space, these spatially embedded networks as two-dimensional lattices. Typically, real spatial networks in two dimensional space are characterized by lower average degree than a square lattice [79]. The case of coupled lattice is not only a representative example for all its universality class but may serve as a lower bound case, while real coupled spatial networks are even more vulnerable.

Here, we review recent analytical and numerical results recently presented by Bashan et al. on the stability of systems of two interdependent spatially embedded networks, modeled as two interdependent lattices [82]. We find that in such systems $q_c = 0$, i.e., any coupling $q > 0$ leads to an abrupt first-order transition. We show that the origin for this extreme vulnerability of spatially embedded networks lies in the critical behavior of percolation of a single lattice, which is characterized by a critical exponent $\beta < 1$ [80,83]. This is in contrast to random networks for which $\beta = 1$, leading to $q_c > 0$ for interdependent random networks. Here the dependency links are between lattices' nodes located in different random spatial positions (Fig. 1a) or between lattice nodes and nodes of random networks where the space does not play a role at all (Fig. 1b). In the case of dependency links between lattice nodes with exactly the same position, the transition is always continuous, as for percolation in a single lattice [69]. Note that the fully interdependent limit of $q = 1$ of coupled lattices was studied by Wei et al. [63].

Our theoretical and numerical approaches predict [82] that a real-world system of interdependent spatially embedded networks which are characterized by $\beta < 1$ will, for any $q > 0$, abruptly disintegrate. Since for percolation of lattice networks it is known that for any dimension $d < 6$, $\beta < 1$ [80], we expect that also interdependent systems embedded in $d = 3$ (or any $d < 6$) will collapse abruptly for any finite fraction of dependency q. Indeed, Dobson et al. [93] analyze the statistics of many real world outages events and show that they are commonly resulted by cascading failure. Our results show that an important possible mechanism in these events is the interdependencies in spatial networks.

Consider a system of two interdependent networks, $i = 1$ and $i = 2$, where a fraction $1-p_i$ of nodes of each network is initially randomly removed. We assume that only the nodes which belong to the giant component of the remaining networks which constitute a fraction $P_{\infty,i}(p_i)$ of the original network remain functional. Each node that has been removed or disconnected from the giant component causes its dependent node in the other network to also fail. This leads to further disconnections in the other network and to cascading failures. The size of the networks' giant components at the end of the cascade is given by $P_{\infty,i}(x_i)$, where x_i are the solutions of the self consistent equations [52]

$$x_1 = p_1 q_1 P_{\infty,2}(x_2) + p_1(1 - q_1) \tag{18}$$

$$x_2 = p_2 q_2 P_{\infty,1}(x_1) + p_2(1 - q_2), \tag{19}$$

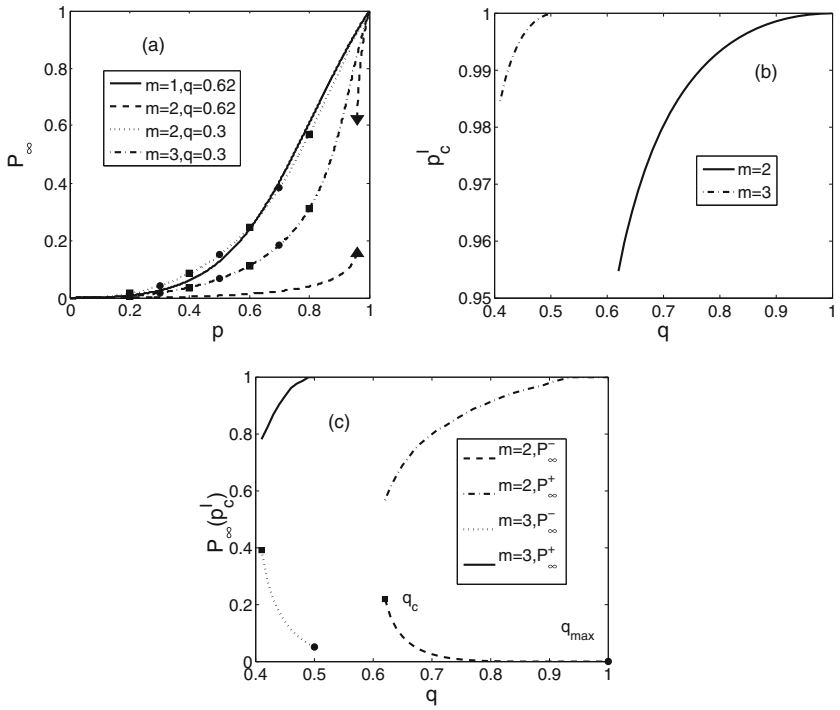

Fig. 1. Results for a RR network formed of SF networks. (a) The giant component P_∞ as a function of p for different values of m and q for $\lambda = 2.5$. (b) The critical threshold p_c^I and (c) the corresponding giant component at the threshold $P_\infty(p_c^I)$ as a function of coupling strength q for $m = 2$ and $m = 3$. The symbols in (a) represent simulation results, obtained by averaging over 20 realizations for $N = 2 \times 10^5$ and number of networks $n = 6$ (squares) and $n = 4$ (circles). The lines represent theoretical results. We can see in (a) that the system shows a hybrid phase transition for $m = 2$ and $q_c < q = 0.62 < q_{\max} = 1/(m-1)$. When $q < q_c$ the system shows a second order phase transition and the critical threshold is $p_c^{II} = 0$. However, in the simulation when p is small (but not zero) $P_\infty = 0$. This happens because $p_c^{II} = 0$ is valid only when the network size $N = \infty$ and $M = \infty$, but in simulations we have finite systems. Furthermore, when $q_c < q < q_{\max}$ the system shows a hybrid transition shown in (a) and (c), and when $q > q_{\max}$ all the networks collapse even if one node fails. We call this hybrid transition because $P_\infty^- > 0$, which is different from the case of ER networks with first order phase transition where $P_\infty^- = 0$. After [71].

where q_i is the fraction of nodes in network i which depends on nodes in the other network. Here we assume no restrictions on the selection of the directed dependency links. The results for the case of "no-feedback-condition", where the dependency links are bidirectional [52], are qualitatively the same. The function $P_{\infty,i}(x)$ can be obtained either analytically or numerically from the percolation behavior of a *single* network.

For simplicity, we focus on a symmetric case, where both networks have the same degree distribution $P(k)$ and same topology, and where $p_1 = p_2 \equiv p$ and $q_1 = q_2 \equiv q$. Still, the results are valid for any system of interdependent spatially embedded networks (like planar graph) which belong to the same universality class. In particular, in order to study the role of spatial embedding, we compare the percolation transition in the case of a pair of interdependent lattices (Fig. 2a) to the case of a pair of interdependent random-regular (RR) networks (Fig. 2c). The RR networks have the

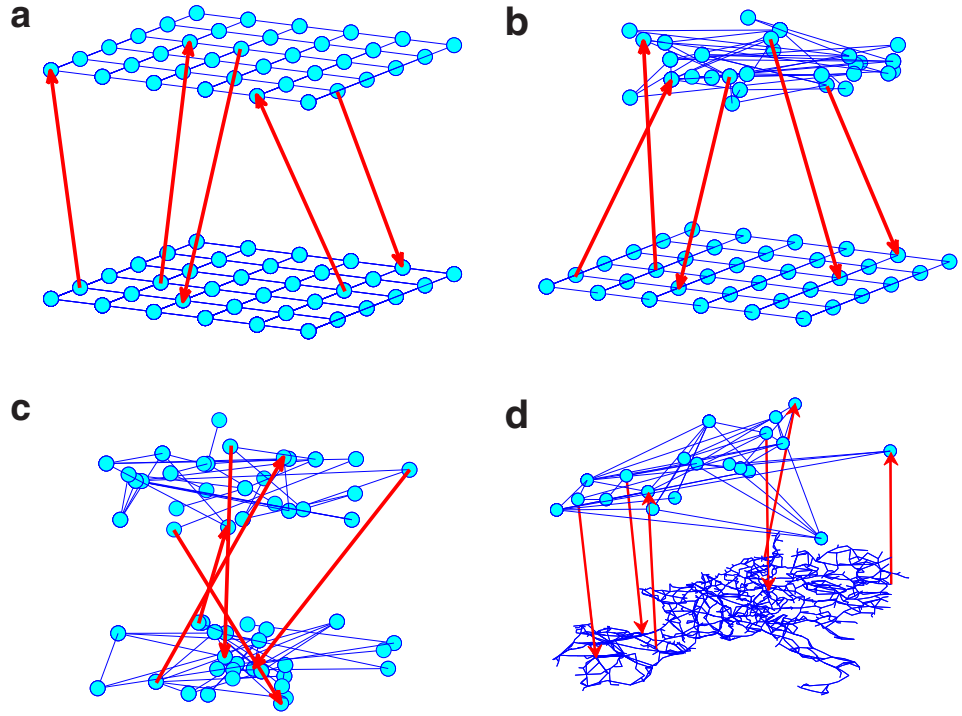

Fig. 2. A system of interdependent networks is characterized by the structure (dimension) of the single networks as well as by the coupling between the networks. In random networks with no space restrictions, such as ER and RR, the connectivity links (blue lines) do not have a defined length. In contrast, in spatially embedded networks nodes are connected only to nodes in their geometrical neighborhood creating a two-dimensional network, modeled here as a square lattice. The (red) arrows represent directed dependency relations between nodes in different networks, which can be of different types: (a) coupled lattices (b) coupled lattice-random network (c) coupled random networks (d) real-world spatial network (European power grid) coupled with random network. Models (b) and (d) belong to the same universality class. After [82].

same degree distribution, $P(k) = \delta_{k,4}$, as for the lattices with the only difference that the lattice-networks are embedded in space, in contrast to RR networks.

In the symmetric case, Eqs. (18) and (19) can be reduced to a single equation

$$x = pqP_\infty(x) + p(1-q), \tag{20}$$

where the size of the giant component at steady state is $P_\infty(x)$. For any values of p and q, the solution of Eq. (20) can be graphically presented as the intersection between the curve $y = pqP_\infty(x) + p(1-q)$ and the straight line $y = x$ representing the right-hand-side and the left-hand-side of Eq. (20) respectively. The form of $P_\infty(x)$ for conventional percolation is obtained from numerical simulations of a single lattice and analytically for a single RR network [61]. From the solution of Eq. (20) we obtain $P_\infty(p)$ as a function of p for several values of q. This $P_\infty(p)$ is the new percolation behavior for a system of interdependent networks, shown in Fig. 4a, for the case of coupled lattices and in Fig. 4b for the case of coupled RR networks. In the case of interdependent lattices, only for $q = 0$, no coupling between the networks (the single network limit), the transition is the conventional second-order percolation transition, while for any $q > 0$ the collapse is abrupt in the form of first-order transition. In

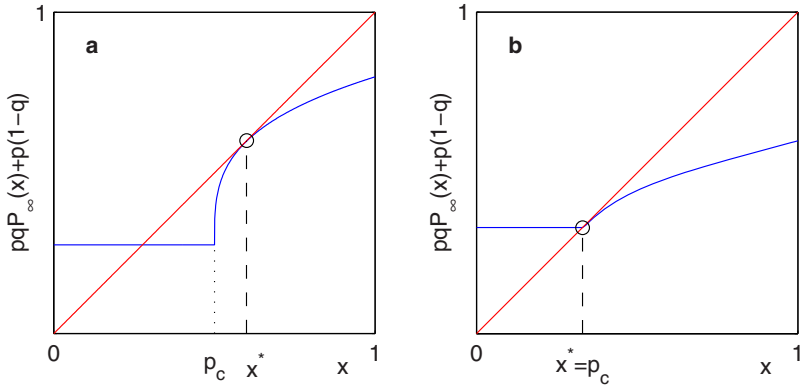

Fig. 3. Schematic solution of the critical point of (a) coupled lattices and (b) coupled random-regular (RR) networks. The left-hand-side and right-hand-side of Eq. (20) are plotted as a straight (red) line and a (blue) curve respectively. The tangential touching point, x^*, marked with a (black) circle, represents the new percolation threshold in the system of interdependent networks. In the case of coupled lattices (panel a), due to the infinite slope of the curve at p_c, x^* is always larger than p_c and, thus, there is always (for any $q > 0$) a discontinuous jump in the size of the giant component as p decreases. In contrast, in coupled random networks (panel b) the slope of the curves is finite for any value of x. Therefore, there exist $q < q_c$ for which x^* is equal to p_c, leading to a continuous behavior in the network's size.

marked contrast, in the case of interdependent RR networks, for $q > q_c \cong 0.43$ the transition is abrupt, while for $q < q_c$ the transition is continuous.

A discontinuity of $P_\infty(p)$ is a result of a discontinuity of $x(p)$, represented graphically as the tangential touching point of the curve and the straight line (see schematic representation in Fig. 3). At this point, $p \equiv p^\star$ is the new percolation threshold in the case of interdependent networks, and $x = x^\star$ yields the size of the giant component at the transition, $P^\star_\infty \equiv P_\infty(x^\star)$, which abruptly jumps to zero as p slightly decreases. The condition for a first-order transition $p = p^\star$, for a given q, is thus given by solving Eq. (20) together with its tangential condition,

$$1 = p^\star q P'_\infty(x^\star). \tag{21}$$

The size of the giant component at the transition $P^\star_\infty$ depends on the coupling strength q such that reducing q leads to smaller value of $x^\star$ and thus smaller discontinuity in the size of the giant component. In general, $P_\infty(x)$ of a single network has a critical threshold at $x = p_c$ such that $P_\infty(x \leqslant p_c) = 0$ while $P_\infty(x > p_c) > 0$ and monotonically increases with x [80]. As long as $x^\star > p_c$, the size of the discontinuity is larger then zero. However, for a certain critical coupling $q \equiv q_c$, $x^\star \to p_c$ and the size of the jump becomes zero. In this case the percolation transition becomes continuous.

Therefore, the critical dependency q_c below which the discontinuous transition becomes continuous, must satisfy Eqs. (20) and (21) for $x \to p_c$ given by

$$p_c = p^\star_c(1 - q_c) \tag{22}$$

$$1 = p^\star_c q_c P'_\infty(p_c). \tag{23}$$

A dramatic different behavior between random and spatial coupled networks is derived from Eq. (23). This difference is a consequence of the critical behavior of percolation in a single network. In the case of a single random network $P'_\infty(x)$ is finite for any value of x. This allows an exact solution of Eq. (23), yielding a finite non-zero value for

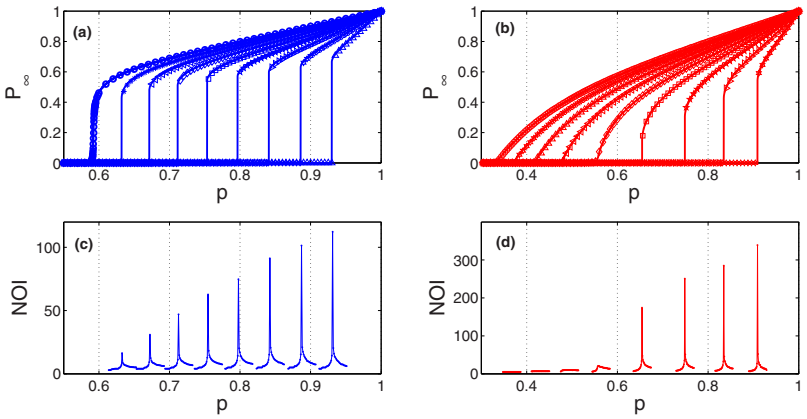

Fig. 4. Percolation transition of interdependent lattices compared to interdependent random networks. The size of the giant component P_∞ at steady state after random failure of a fraction $1-p$ of the nodes of (a) two interdependent lattice networks with periodic boundary conditions (PBC) and (b) two random-regular (RR) networks. All networks are of size 16×10^6 nodes and the same degree distribution $P(k) = \delta_{k,4}$. The coupling between the lattices and between the RR networks changes from $q = 0$ to $q = 0.8$ with step 0.1 (from left to right). The solid lines are the solutions of Eq. (20) and the symbols represent simulation results. In the case of interdependent lattices, only for $q = 0$ (no coupling, i.e., a single lattice) the transition is the conventional second-order percolation, while for any $q > 0$ the collapse is abrupt in the form of first-order transition. This is in marked contrast to the case of interdependent RR networks, where only for $q > q_c \cong 0.43$ the transition is abrupt, while for $q < q_c$ the transition is continuous. A characteristic behavior in a first-order percolation transition in coupled networks is the sharp divergence of the number of iterations (NOI) when p approaches $p_c^\star$ [60] as seen for (c) coupled lattices for any $q > 0$ and for (d) coupled RR networks for $q > q_c$. Models of coupled lattices with PBC have the same behavior as models without. After [82].

q_c. However, for the case of a single lattice network the derivative of $P_\infty(x)$ diverges at the critical point, $P'_\infty(p_c) = \infty$, yielding $q_c = 0$. Therefore, from Eq. (23) follows that any coupling $q > 0$ between lattices leads to an abrupt first order transition, as indeed suggested by simulations reported in Fig. 4.

The behavior of the percolation order parameter of a single network near the critical point is defined by the critical exponent β, where $P_\infty(x \to p_c) = A(x - p_c)^\beta$. Since for single 2d lattice $\beta = 5/36 < 1$, it follows that $P'_\infty(x)$ diverges for $x \to p_c$ for all networks embedded in two dimensional space [80,83]. In contrast, for random networks, such as Erdös-Rényi (ER) and Random-Regular (RR), $\beta = 1$ which yields a finite value of $P'_\infty(p_c)$ [80,83] and therefore a finite value for q_c.

4 Attack strategies

The resilience of a complex network to random attack or to malicious attacks based on targeting special nodes (by degree, betweenness etc.) has been studied extensively in recent years [4,5,13,84]. It has been shown that the robustness of the network under such an attack is highly dependent on it topology. Resilience to geographic localized attacks has been studied for a number of scenarios and on specific single networks [85–87]. Currently, a general theoretical approach of geographically localized attacks that considers the effects of cascading failures due to interactions between networks is being developed [88]. Indeed localized attacks with positive feedback caused

by interdependencies has been shown to have catastrophic consequences such as in the 2003 Italian blackout [45,47].

4.1 Targeted attacks

In real-world scenarios, initial system failures seldom occur randomly and can be the result of targeted attacks on central nodes. Such attacks can also occur in less central nodes in an effort to circumvent central node defenses, e.g., heavily-connected Internet hubs tend have more effective firewalls. Targeted attacks on high degree nodes [4,6,7,13,43] or high betweenness nodes [89] in *single* networks dramatically affect their robustness. To study the targeted attack problem on interdependent networks [13,57,90–92] we assign a value $W_\alpha(k_i)$ to each node, which represents the probability that a node i with k_i degree will be initially attacked and become inactive, i.e.,

$$W_\alpha(k_i) = \frac{k_i^\alpha}{\sum_{i=1}^{N} k_i^\alpha}, -\infty < \alpha < +\infty. \tag{24}$$

When $\alpha > 0$, higher-degree nodes are more vulnerable to intentional attack. When $\alpha < 0$, higher-degree nodes are less vulnerable and have a have a lower probability of failure. The case $\alpha = 0$, $W_0 = \frac{1}{N}$, represents the random removal of nodes [45].

In the interdependent networks model with networks A and B described in Ref. [45], a fraction $1 - p$ of the nodes from one network are removed with a probability $W_\alpha(k_i)$ [Eq. (24)]. After this removal, the cascading failures are the same as those described in Ref. [45]. To analytically solve the targeted attack problem, Huang et al. [57] developed 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 [57,92].

4.2 Localized attacks

Modern critical infrastructures are embedded in space and have extensive interdependencies [48,49,51,79]. Entities in one network (e.g., power generation/distribution, communications, transportation, etc.) are dependent upon entities in another and failures in one network can trigger failures in another. It has been shown that these dependencies lead to substantially decreased robustness and can even yield abrupt first order transitions which are absent in isolated networks [45–47,51,52,54,59,69,70,82]. Spatially embedded interdependent networks have been studied under *random* attack, where a new kind of abrupt collapse is found. This collapse is characterized by the spreading of cascading failures and requires a finite fraction of nodes to be removed [63,82]. However, a purely *random* failure of a finite fraction of nodes in a very large network can be unrealistic. A more realistic scenario is a failure of group of neighboring nodes due to a natural disaster like the 2011 Tōhoku earthquake and tsunami or due to a malicious attack affecting all networks in a given region (e.g., a nuclear strike) or only certain infrastructures (e.g., an electromagnetic pulse or chemical/biological attack). The resilience of a system of interdependent networks to an attack of this sort, which we call "localized attack," has not been addressed before.

Recent work has suggested a new type of targeted attacks. Berezin et al. [88] show that there exists a critical damage size with radius r_h^c, above which localized damage will spread and destroy the entire system and below which the damage will remain in place. This critical size is determined solely by intensive system quantities and thus, in contrast to random failures, constitutes a zero-fraction of the system in the limit of large systems ($N \to \infty$).

4.3 The affect of modular structure on network resilience

Network science has become a leading approach to the study of emergent collective phenomena in complex systems, with a wide range of applications to fundamental real word systems [44]. Much research has focused on the function of networks, mainly their resilience and stability to attacks [34], and the structure of networks, mainly in terms of communities, or modules, in networks [94]. Many real world systems have been shown to exhibit a modular structure, which is key to their behavior and functioning. For example, recent studies of biological networks show that the deletion of nodes connecting between modules can have a deleterious effect on the network integrity [95], efficiency [96,97], and stability [98].

Some of the structural properties that have been found to play a very important role recently have been the existence of communities, cliques, in networks, and the modular organization of networks. The modular structures or communities have been shown to be relevant in our current understanding of the structure and dynamics of complex systems. Detecting communities is of great importance in sociology, biology and computer science, disciplines where systems are often represented as graphs. This problem has been found to be difficult and not yet satisfactorily solved, despite the huge effort of a large interdisciplinary community of scientists working on it over the past few years, Communities could also be considered in the new frameworks of interdependent and multiplex networks [99].

Shai et al. [99] have presented the first theoretical description of the effect of modular structure on the function and resilience of networks. To this end, they investigated the percolation process on networks consisting of a varying number of modules, m, when attacking the interconnected high betweenness nodes. The analytical solution reveals two percolation regimes separated by a critical number of modules m^*: for $m < m^*$ one needs to remove all interconnected nodes to break the system, while the remaining modules are almost not affected internally. This regime is characterized by an abrupt first order percolation transition. In contrast, for $m > m^*$ one needs to remove only a fraction of the interconnected nodes, and consequently the system continuously collapses. This is due to the fact that for $m > m^*$ the number of interconnected nodes is high and partial removal of these already breaks the modules internally, and thus enhancing the collapse of the whole system.

The analytical and numerical investigation of the effect of modularity on network stability has important implications for real world networks, such as cognitive and neural brain networks. The modular architecture of neural structural and functional networks is considered a fundamental principle of the brain. This non-random modular architecture is crucial for the brain's functional demands of segregation and integration of information. In fact, disrupted brain modular organization is related to neuropathology, such as schizophrenia, autism, Alzheimer's and impulsivity. At the cognitive level (the level of information processing in the brain), network analysis is mainly focused on language and memory networks; however, the effect of modularity and its importance in cognitive network organization is still unclear. Thus, this work provides the first analytical and simulation evidence into the effect of modularity on network resilience and vulnerability. These results have many real world applications, from the optimal design of infrastructure, new insights and understandings of brain disorders, and efficient immunization approach in modular networks, where epidemic spreading can be prevented at a low cost by immunizing interconnected nodes.

5 Repair, recovery, and optimization of networks and networks of networks

In this section we present two theoretical frameworks recently developed, which can be applied to promote repair and recovery in networks and networks of networks. While

the two frameworks have been developed for single networks, they are currently being expanded to the case of interdependent network of networks, with and without spatial constraints.

5.1 Repair and optimization strategies

Recently, Schneider et al. [34] have developed an efficient mitigation method and discovered that with relatively minor modifications in the topology of a given network and without increasing the overall length of connections, it is possible To mitigate considerably the danger of malicious attacks. The presented efficient mitigation method against malicious attacks is based on Developing and introducing a unique measure for robustness. The authors show that the common measure for robustness of networks in terms of the critical fraction of attacks at which the system completely Collapses, the percolation threshold, may not be useful in certain scenarios. This measure, for example, ignores situations in which the network suffers a significant damage, but still Keeps its integrity. Besides the percolation threshold, there are other robustness measures based, for example, inHans the shortest path, or on the graph spectrum. However, these are less frequently used for being too complex or less intuitive. In contrast, the unique robustness measure presented by Schneider et al. [34], which considers the size of the largest component during all possible malicious attacks, is as simple as possible and only as complex as necessary. The robustness measure is defined as

$$R = \frac{1}{N}\sum s(q), \tag{25}$$

where N is the number of nodes in the network, and $s(q)$ is the fraction of nodes in the largest connected cluster after removing a fraction q of nodes. The normalization factor $1/N$ ensures that the robustness of networks with different sizes is comparable. The range of values for R is between $1/N$ and 0.5, where these limits correspond, respectively, to a star network and a fully connected network.

In Fig. 5A and Fig. 5B we show the backbone of the European Union (EU) power grid and the location of the European PoP and their respective vulnerability in Fig. 5C and Fig. 5D. The dotted lines in Fig. 5C and Fig. 5D represent the size of the largest connected component of the networks after a fraction q of the most connected nodes have been removed. Instead of using the static approach to find the q most connected nodes at the beginning of the attack, we use a dynamical approach. In this case the degrees are recalculated during the attack, which corresponds to a more harmful strategy. As a consequence, in their current structure, the shutdown of only 10% of the power stations and a cut of 12% of PoP would cause 90% of nodes to fail.

To avoid such a dramatic breakdown and reduce the fragility of these networks, here we propose a strategy that modifies only a small number of power lines or cables without increasing the total length of the links (limiting cost) and the number of links of each node. These small local changes not only mitigate the efficiency of malicious attacks, but at the same time preserve the functionality of the system. In Figs. 5C and D the robustness of the original networks are given by the areas under the dashed curves, whereas the areas under the solid lines correspond to the robustness of the improved networks. Therefore, the green areas in Figs. 5C and D demonstrate the significant improvement of the resilience of the network for any fraction q of attack. This means that terrorists would cause less damage or they would have to attack many more power stations, and hackers would need to attack more PoP to significantly damage the system.

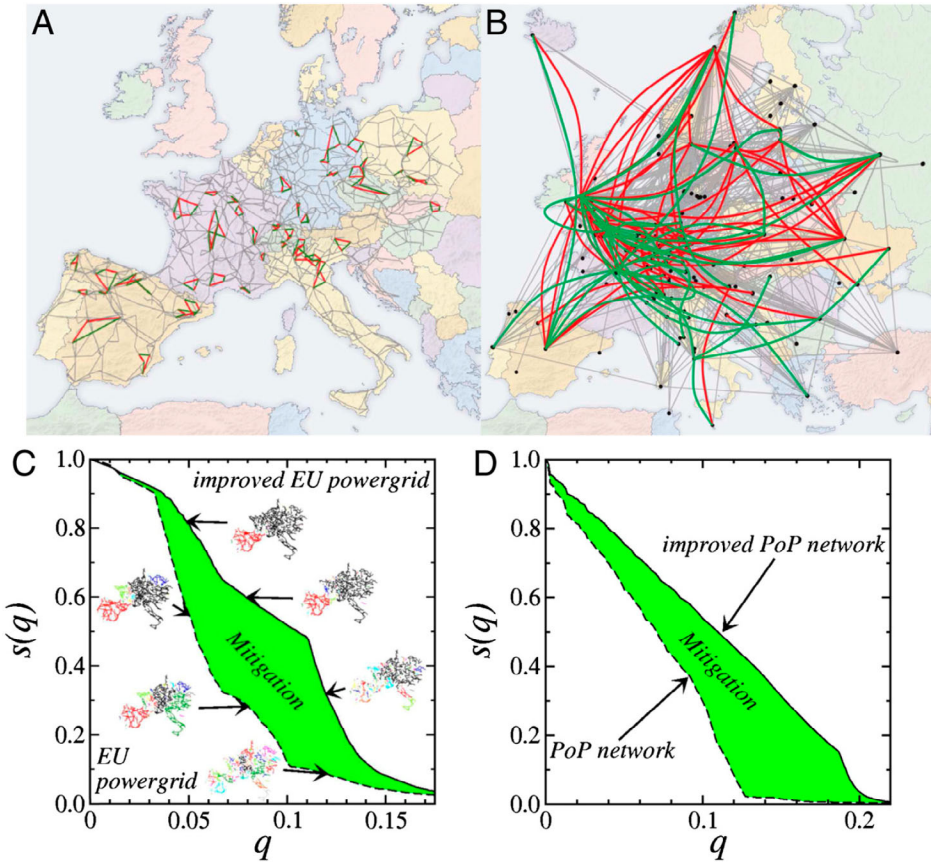

Fig. 5. Mitigation of malicious attacks on the power supply system in Europe and the global Internet at the level of service providers. In (A) we show the EU power grid with $N = 1254$ generators and $M = 1811$ power lines and in (B) the Internet with $N = 1098$ service providers and $M = 6089$ connection among them, where only the European part is shown. The red edges correspond to the 5% connections that we suggest to replace by the green ones. The network fragmentation under a malicious attack is shown for (C) EU power generators and for (D) PoP. The dashed lines in (C) and (D) corresponds to the size of the largest component in each original system and the solid lines to typical redesigned networks after changing 5% of the connections. The green areas give the mitigation of malicious attack, which correspond to improving robustness by 45% for the EU power grid and 55% for the PoP. After [34].

5.2 Recovery in networks

Although some research has focused on the transient dynamics as failure propagation, there is an entire class of real-world dynamic complex systems in which networks can spontaneously recover after their collapse, and the mechanism for this network global recovery has not yet been adequately understood. The Internet can initially fail after a severe attack and then, after a period of time, recover. A human brain can spontaneously recover after an epileptic attack. A traffic network returns to its normal state after a period of gridlock. A financial network may, after a period of time, recover after having a large fraction its constituents fail.

Recently, Majdandzic et al. [100] developed a framework for understanding dynamic networks that demonstrate an ability to spontaneously recover. It is assumed that any node in the network can fail independently of other nodes (internal failure) with a probability of $p\ dt$ during a time interval $dt = 1$. Next, it is assumed that any node can fail due to external causes, e.g., if it has a substantially damaged neighborhood. A simple threshold rule is used to define a *substantially damaged* neighborhood: it is a neighborhood containing fewer than or equal to m active nodes, where m is an integer. If node j has more than m active neighbors during dt, its neighborhood is "healthy", but if node j has $< m$ active neighbors during the interval dt, there is a probability $r\ dt$ that node j will externally fail. Finally, we assume that there is a reversal process, a recovery from failures. Node j recovers from an *internal* failure after a time period $\tau \neq 0$, and it recovers from an *external* failure after time τ'. For simplicity, we set $\tau' = 1$. If there are no recoveries ($\tau = \tau' = \infty$) the system reduces to the Watts model [1] generalized and rigorously solved in Ref. [101]. We find that introducing dynamic recovery leads to spontaneous network collapse and recovery – the phase switching phenomena. Furthermore, by varying the parameters an interesting phase diagram can be obtained showing two phases of stable and unstable regimes as well metastable regime where hysteresis behavior can be observed.

This framework presents a possible methodology to promote recovery in real world networks and network of networks. Since the results presented by Majdandzic et al. [100] demonstrate that with the presence of a probability of recovery, the network can flip from active to inactive states. Thus, in the case of attacks on specific parts of the network and decline in network functionality, repairing specific nodes in the network could sufficiently initiate the flipping of the network back into an active state. Thus, we propose this methodology as a repair strategy for real world networks under attack.

6 Summary and future outlook

The current challenges in network theory are the need to develop a new framework to deal with such coupled and interdependent systems, where not only the structural properties are considered, but dynamic and spatial considerations, as well as coupling and dependency between networks are also taken into account. The employment of ideas and techniques from complex network theory and the proposed theory of coupled and interdependent networks to understand and quantify the role of connections and dependencies within a system and between different ones opens the possibility to manage and control the complexity, optimize the systems structure and function and reduce their vulnerability to failures and mitigate the effects of different attack strategies. At the technological level, such understanding will help in developing smart infrastructures that are able to predict and adjust to different conditions and able to respond successfully in real time to abnormal load shedding, thus avoiding, for example, blackouts, traffic jams, or inefficiencies and shortages in the supply of oil and gas. The commercial and industrial systems strongly require an efficient and resilient logistic network to avoid excessive inventories and the lack of robustness against cyclic perturbations, which affect the production costs and, consequently, the competitiveness. In social systems, the new network science will enable early identification of social crises, and provide methods to mitigate social catastrophes. As our society is dependent on a large variety of infrastructure, it has become crucial to identify and understand the affect of different attack strategies, and how they affect the targeted network, and then propagate to other coupled and dependent networks. Such understanding would then be integrated with repair strategies, as discussed in section 5, to develop strategies for a fast and efficient repair of the system. Thus, the

aim of this paper was to review both sides of this coin – attack and repair strategies – which would result in resilient and sustainable infrastructure for the daily functioning in the modern socio-techno-economic world.

SH, HES, AB and DYK thank DTRA, ONR, BSF, the LINC (No. 289447) and the Multiplex (No. 317532) EU projects, the DFG, and the Israel Science Foundation for support. JXG thanks the support from National Natural Science Foundation of China (Grants No. 61374160) for support.

References

1. D.J. Watts, S.H. Strogatz, Nature **393**(6684), 440 (1998)
2. A.L. Barabási, R. Albert, Science **286**(5439), 509 (1999)
3. M. Faloutsos, P. Faloutsos, C. Faloutsos, in *ACM SIGCOMM Computer Communication Review*, Vol. 29 (ACM, 1999), p. 251
4. R. Albert, H. Jeong, A.L. Barabási, Nature **406**(6794), 378 (2000)
5. R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Phys. Rev. Lett. **85**(21), 4626 (2000)
6. D.S. Callaway, M.E. Newman, S.H. Strogatz, D.J. Watts, Phys. Rev. Lett. **85**(25), 5468 (2000)
7. R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Phys. Rev. Lett. **86**(16), 3682 (2001)
8. R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, U. Alon, Sci. Signal. **298**(5594), 824 (2002)
9. D.J. Watts, Proc. Natl. Acad. Sci. USA **99**(9), 5766 (2002)
10. M.E.J. Newman, SIAM Rev. **45**(2), 167 (2003)
11. A. Barrat, M. Barthelemy, R. Pastor-Satorras, A. Vespignani, Proc. Natl. Acad. Sci. USA **101**(11), 3747 (2004)
12. M.E.J. Newman, M. Girvan, Phys. Rev. E **69**(2), 026113 (2004)
13. L.K. Gallos, R. Cohen, P. Argyrakis, A. Bunde, S. Havlin, Phys. Rev. Lett. **94**(18), 188701 (2005)
14. V. Latora, M. Marchiori, Phys. Rev. E **71**(1), 015103 (2005)
15. C. Song, S. Havlin, H.A. Makse, Nature **433**(7024), 392 (2005)
16. S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.U. Hwang, Phys. Rep. **424**(4), 175 (2006)
17. M.E.J. Newman, A.L. Barabasi, D.J. Watts, *The Structure and Dynamics of Networks* (Princeton University Press, 2011)
18. B.J. West, P. Grigolini, *Complex Webs: Anticipating the Improbable* (Cambridge University Press, 2010)
19. G. Bonanno, G. Caldarelli, F. Lillo, R.N. Mantegna, Phys. Rev. E **68**(4), 046130 (2003)
20. D. Li, K. Kosmidis, A. Bunde, S. Havlin, Nat. Phys. **7**(6), 481 (2011)
21. D.Y. Kenett, M. Tumminello, A. Madi, G. Gur-Gershgoren, R. Mantegna, E. Ben-Jacob, PloS one **5**(12), e15032 (2010)
22. D.Y. Kenett, T. Preis, G. Gur-Gershgoren, E. Ben-Jacob, Int. J. Bifurc. Chaos **22**(7), 1250181 (2012)
23. Y.N. Kenett, D.Y. Kenett, E. Ben-Jacob, M. Faust, PloS one **6**(8), e23912 (2011)
24. A. Madi, D. Kenett, S. Bransburg-Zabary, Y. Merbl, F. Quintana, S. Boccaletti, A. Tauber, I. Cohen, E. Ben-Jacob, Chaos **21**(1), 016109 (2011)
25. S. Bransburg-Zabary, D.Y. Kenett, G. Dar, A. Madi, Y. Merbl, F.J. Quintana, A.I. Tauber, I.R. Cohen, E. Ben-Jacob, Phys. Biol. **10**(2), 025003 (2013)
26. J.S. Andrade Jr., H.J. Herrmann, R.F.S. Andrade, L.R. Da Silva, Phys. Rev. Lett. **94**, 018702 (2005)
27. M. Kitsak, L.K. Gallos, S. Havlin, F. Liljeros, L. Muchnik, H.E. Stanley, H.A. Makse, Nat. Phys. **6**, 888 (2010)
28. E. López, S.V. Buldyrev, S. Havlin, H.E. Stanley, Phys. Rev. Lett. **94**(24), 248701 (2005)

29. M. Boguná, D. Krioukov, Phys. Rev. Lett. **102**(5), 058701 (2009)
30. V. Colizza, A. Barrat, M. Barthelemy, A. Vespignani, et al., Proc. Natl. Acad. Sci. USA, 103 (2005)
31. Z. Wu, L.A. Braunstein, V. Colizza, R. Cohen, S. Havlin, H.E. Stanley, Phys. Rev. E **74**(5), 056104 (2006)
32. R. Albert, A.L. Barabási, Rev. Mod. Phys. **74**(1), 47 (2002)
33. A. Bunde, S. Havlin, *Fractals and Disordered Systems* (Springer, Berlin, Heidelberg, 1991)
34. C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Proc. Natl. Acad. Sci. USA **108**(10), 3838 (2011)
35. Y. Chen, G. Paul, S. Havlin, F. Liljeros, H.E. Stanley, Phys. Rev. Lett. **101**(5), 058701 (2008)
36. R. Cohen, S. Havlin, D. Ben-Avraham, Phys. Rev. Lett. **91**(24), 247901 (2003)
37. L.A. Braunstein, S.V. Buldyrev, R. Cohen, S. Havlin, H.E. Stanley, Phys. Rev. Lett. **91**(16), 168701 (2003)
38. R. Pastor-Satorras, A. Vespignani, Phys. Rev. Lett. **86**(14), 3200 (2001)
39. D. Balcan, V. Colizza, B. Gonçalves, H. Hu, J.J. Ramasco, A. Vespignani, Proc. Natl. Acad. Sci. USA **106**(51), 21484 (2009)
40. G. Palla, I. Derényi, I. Farkas, T. Vicsek, Nature **435**(7043), 814 (2005)
41. G. Kossinets, D.J. Watts, Science **311**(5757), 88 (2006)
42. M.E.J. Newman, Proc. Natl. Acad. Sci. USA **98**(2), 404 (2001)
43. A.A. Moreira, J.S. Andrade Jr., H.J. Herrmann, J.O. Indekeu, Phys. Rev. Lett. **102**(1), 018701 (2009)
44. S. Havlin, D.Y. Kenett, E. Ben-Jacob, A. Bunde, R. Cohen, H. Hermann, J. Kantelhardt, J. Kertész, S. Kirkpatrick, J. Kurths, et al., Eur. Phys. J. Special Topics **214**(1), 273 (2012)
45. S. Buldyrev, R. Parshani, G. Paul, H. Stanley, S. Havlin, Nature **464**(7291), 1025 (2010)
46. R. Parshani, S.V. Buldyrev, S. Havlin, Phys. Rev. Lett. **105,** 048701 (2010)
47. V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, R. Setola, Int. J. Crit. Infrastruct. **4**, 63 (2008)
48. J. Peerenboom, R. Fischer, R. Whitfield, in *Proc. CRIS/DRM/IIIT/NSF Workshop Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures* (2001)
49. S. Rinaldi, J. Peerenboom, T. Kelly, IEEE Control. Syst. Magn. **21**, 11 (2001)
50. R. Cohen, S. Havlin, *Complex Networks: Structure, Robustness and Function* (Cambridge University Press, 2010)
51. A. Vespignani, Nature **464**, 984 (2010)
52. J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Phys. Rev. Lett. **107**, 195701 (2011)
53. E.A. Leicht, R.M. D'Souza, Preprint at `http://arxiv.org/abs/0907.0894` (2009)
54. C.D. Brummitt, R.M. D'Souza, E.A. Leicht, Proc. Natl. Acad. Sci. **109**, 680 (2012)
55. J. Hao, S. Cai, Q. He, Z. Liu, Chaos **21**, 016104 (2011)
56. A. Bashan, R.P. Bartsch, J.W. Kantelhardt, S. Havlin, P.C. Ivanov, Nat. Commun. **3**, 702 (2012)
57. X. Huang, J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Phys. Rev. E (R) **83**, 065101 (2011)
58. S.V. Buldyrev, N.W. Shere, G.A. Cwilich, Phys. Rev. E **83**, 016112 (2011)
59. Y. Hu, B. Ksherim, R. Cohen, S. Havlin, Phys. Rev. E **84**, 066116 (2011)
60. R. Parshani, S.V. Buldyrev, S. Havlin, Proc. Natl. Acad. Sci. USA **108**, 1007 (2011)
61. A. Bashan, R. Parshani, S. Havlin, Phys. Rev. E **83**, 051127 (2011)
62. C.M. Schneider, N. Yazdani, N.A.M. Araujo, S. Havlin, H.J. Herrmann, Sci. Rep. **3**, 1969 (2013)
63. W. Li, A. Bashan, S.V. Buldyrev, H.E. Stanley, S. Havlin, Phys. Rev. Lett. **108**, 228702 (2012)
64. P. Erdös, A. Rényi, Publ. Math. Debrecen **6**, 290 (1959)
65. P. Erdös, A. Rényi, Publ. Math. Inst. Hungar. Acad. Sci. **5**, 1761 (1960)

66. B. Bollobas, *Graph Theory* (North Holland, 1982)
67. D.Y. Kenett, J. Gao, X. Huang, S. Shao, I. Vodenska, S.V. Buldyrev, G. Paul, H.E. Stanley, S. Havlin, in *Networks of Networks: The Last Frontier of Complexity* (Springer International Publishing, 2014), p. 3
68. J. Gao, S.V. Buldyrev, S. Havlin, H.E. Stanley, Phys. Rev. E **85**, 066134 (2012)
69. S. Son, P. Grassberger, M. Paczuski, Phys. Rev. Lett. **107**, 195702 (2011)
70. J. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Nat. Phys. **8**, 40 (2012)
71. J. Gao, S.V. Buldyrev, H.E. Stanley, X. Xu, S. Havlin, Phys. Rev. E **88**, 062816 (2013)
72. D. Zhou, A. Bashan, R. Cohen, Y. Berezin, N. Shnerb, S. Havlin, Phys. Rev. E **90**, 012803 (2014)
73. L.D. Valdez, P.A. Macri, H.E. Stanley, L.A. Braunstein, Phys. Rev. E(RC) **88**, 050803(R) (2013)
74. L.D. Valdez, P.A. Macri, L.A. Braunstein, J. Phys. A: Math. Theor. **47**, 055002 (2014)
75. R. Milo, S. Shen-Orr, S. Itzkovitz, N. Kashtan, D. Chklovskii, U. Alon, Science **298**, 824 (2002)
76. U. Alon, Science **301**, 1866 (2003)
77. R. Khanin, E. Wit, J. Comput. Biol. **13**, 810 (2006)
78. S.N. Dorogovtsev, J.F.F. Mendes, *Evolution of Networks: From Biological Nets to the Internet and WWW* (Physics) (Oxford University Press, 2003)
79. M. Barthelemy, Phys. Rep. **499**, 1 (2011)
80. A. Bunde, A.S. Havlin, *Fractals and Disordered Systems* (Springer, New York, 1991)
81. D. Li, K. Kosmidis, A. Bunde, S. Havlin, Nature Phys. **7**, 481 (2011)
82. A. Bashan, Y. Berezin, S.V. Buldyrev, S. Havlin, Nat. Phys. **9**, 667 (2013)
83. D. Stauffer, A. Aharony, *Introduction to Percolation Theory*, 2nd revised edition (Taylor & Francis, 2003), p. 25
84. D.S. Callaway, J.E. Hopcroft, J.M. Kleinberg, M.E.J. Newman, S.H. Strogatz, Phys. Rev. E **64**, 041902 (2001)
85. S. Naumayer, G. Zussman, R. Cohen, E. Modiano, Networking, IEEE/ACM Trans. **19**, 1610 (2011)
86. P.K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, G. Zussman, Military Communications Conference, 2010-MILCOM 2010. IEEE (2010)
87. P.K. Agarwal, A. Efrat, S. Ganjugunte, D. Hay, S. Sankararaman, G. Zussman, Infocom (2011)
88. Y. Berezin, A. Bashan, M.M. Danziger, D. Li, S. Havlin [arXiv:1310.0996] (2013)
89. P. Holme, B.J. Kim, C.N. Yoon, S.K. Han, Phys. Rev. E. **65**, 056109 (2002)
90. T. Tanizawa, S. Havlin, H.E. Stanley, Phys. Rev. E **85**, 046109 (2012)
91. X. Huang, S. Shao, H. Wang, S.V. Buldyrev, H.E. Stanley, S. Havlin, EPL **101**, 18002 (2013)
92. G. Dong, J. Gao, R. Du, L. Tian, H.E. Stanley, S. Havlin, Phys. Rev. E **87**, 052804 (2013)
93. I. Dobson, B.A. Carreras, V.E. Lynch, D.E. Newman, Chaos **17**, 026103 (2007)
94. M.E.J. Newman, Proc. Natl. Acad. Sci. USA **103**, 8577 (2006)
95. J.D.J. Han, N. Bertin, T. Hao, D.S. Goldberg, G.F. Berriz, L.V. Zhang, D. Dupuy, A.J.M. Walhout, M.E. Cusick, F.P. Roth, M. Vidal, Nature **430**, 88 (2004)
96. L.K. Gallos, M. Sigman, H.A. Makse, Front. Physiol. **3** (2012)
97. O. Sporns, C.J. Honey, R. Kotter, PLoS ONE **2**, e1049 (2007)
98. Y. He, J. Wang, L. Wang, Z.J. Chen, C. Yan, H. Yang, H. Tang, C. Zhu, Q. Gong, Y. Zang, A.C. Evans, PLoS ONE **4**, e5226 (2009)
99. S. Shai, D.Y. Kenett, Y.N. Kenett, M. Faust, S. Dobson, S. Havlin [arXiv:1404.4748] (2014)
100. A. Majdandzic, B. Podobnik, S.V. Buldyrev, D.Y. Kenett, S. Havlin, H.E. Stanley, Nat. Phys. **10**(1), 34 (2014)
101. J.P. Gleeson, D.J. Cahalane, Proc. SPIE 6601, *Noise and Stochastics in Complex Systems and Finance*, 66010W (2007)