



# Vulnerability and controllability of networks of networks



Xueming Liu<sup>a,b</sup>, Hao Peng<sup>c</sup>, Jianxi Gao<sup>d,\*</sup>

<sup>a</sup> Key Laboratory of Image Information Processing and Intelligent Control, School of Automation, Huazhong University of Science and Technology, Wuhan 430074, Hubei, PR China

<sup>b</sup> Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA

<sup>c</sup> Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua 321004, Zhejiang, PR China

<sup>d</sup> Center for Complex Network Research and Department of Physics, Northeastern University, Boston, MA 02115, USA

## ARTICLE INFO

### Article history:

Available online 7 September 2015

## ABSTRACT

Network science is a highly interdisciplinary field ranging from natural science to engineering technology and it has been applied to model complex systems and used to explain their behaviors. Most previous studies have been focus on isolated networks, but many real-world networks do in fact interact with and depend on other networks via dependency connectivities, forming “networks of networks” (NON). The interdependence between networks has been found to largely increase the vulnerability of interacting systems, when a node in one network fails, it usually causes dependent nodes in other networks to fail, which, in turn, may cause further damage on the first network and result in a cascade of failures with sometimes catastrophic consequences, e.g., electrical blackouts caused by the interdependence of power grids and communication networks. The vulnerability of a NON can be analyzed by percolation theory that can be used to predict the critical threshold where a NON collapses. We review here the analytic framework for analyzing the vulnerability of NON, which yields novel percolation laws for  $n$ -interdependent networks and also shows that percolation theory of a single network studied extensively in physics and mathematics in the last 50 years is a specific limited case of the more general case of  $n$  interacting networks. Understanding the mechanism behind the cascading failure in NON enables us finding methods to decrease the vulnerability of the natural systems and design of more robust infrastructure systems. By examining the vulnerability of NON under targeted attack and studying the real interdependent systems, we find two methods to decrease the systems vulnerability: (1) protect the high-degree nodes, and (2) increase the degree correlation between networks. Furthermore, the ultimate proof of our understanding of natural and technological systems is reflected in our ability to control them. We also review the recent studies and challenges on the controllability of networks and temporal networks.

© 2015 Elsevier Ltd. All rights reserved.

## 1. Introduction

Many real-world complex systems can be modeled as complex networks, and it has attracted the attention of scientists and engineers studying such wide-ranging topics as power grid systems, computer science, biology, and social

science [1–21]. Plenty of studies have been carried on the structural and dynamic properties of real-world networks, and most networks are found to show a power-law degree distribution and scale-free (SF), e.g. Internet [22], the WWW [3], social networks [23–28], infrastructure networks [29], biological networks [30,31] etc. Comparing to the classical Erdős-Rényi (ER) networks [32], SF networks are significantly more robust than ER networks to random failures but more vulnerable to targeted attack [3–5,33].

\* Corresponding author. Tel.: +16178889526.

E-mail address: [jianxi.gao@gmail.com](mailto:jianxi.gao@gmail.com) (J. Gao).

The vulnerability of a network characterizes its inability to withstand the effects of node or link failures. On the opposite direction, the ability of a network to remain functional after initial attack (called robustness) either can be characterized by the integral size of the giant connected component during a whole attacking period [34,35] or defined by the percolation thresholds [4,36,37]. The percolation threshold,  $p_c$ , is the critical fraction of remaining nodes (or links) that leads to the collapse of the network [4,38], which is usually predicted by using percolation theory, a method from statistical physics [38,39]. Moreover, using percolation theory one can address some other issues, such as efficient attacks or immunization [5,8,33,40,41], obtaining optimal path [42] and designing robust networks [34,43]. The study of the vulnerability or the robustness of complex systems can help us understand the real-world and enable us to make the infrastructures we use in everyday life more efficient and more robust.

It is increasingly clear that diverse critical infrastructures are not isolated but coupled together or depend on each other, such as water and food supply, communications, fuel, financial transactions, and power stations [44–50]. Take a coupled system for example, as shown in Fig. 1, the electric power network provides power for pumping and for controlling systems of water network, the water network provides water for cooling and emissions reduction of power network, the fuel network provides fuel for generators for the electric power network and the electric power network provides power to pump oil for fuel network, etc [51,52]. The interdependence between networks can highly increase the vulnerability of the system, since failure of nodes in one network may lead to the failure of dependent nodes in other networks and this may happen recursively and lead to a cascade of failures and system collapse. For example, electrical blackouts that affect large regions are cascading failures caused by the interdependence between two systems: communication network and power grid [49,53].

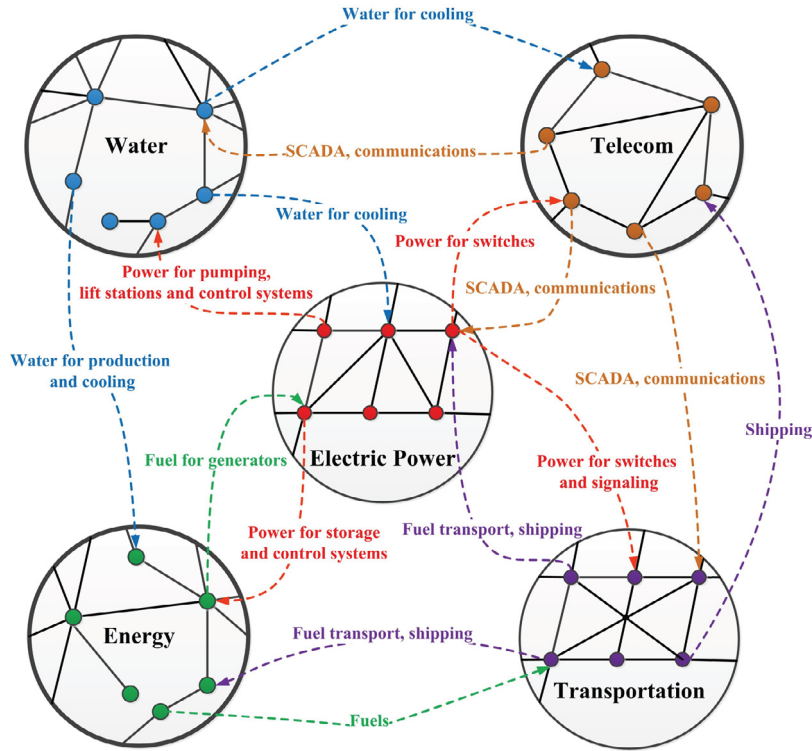
The interactions between systems have led to an emerging new field in network science that focuses on what are variously called interdependent networks [54–64], interconnected networks [65–67], multi-layered networks [68–72], multiplex networks [73], and in general a network of networks [37,50,74,75]. In these systems, networks interact with each other and exhibit structural and dynamical features that differ from those observed in isolated networks. For example, Buldyrev et al. [54] developed an analytical framework based on the generating function formalism [76,77], describing the cascading failures in two interdependent networks, and finding a first order discontinuous phase transition, and this is dramatically different from the second order continuous phase transition found in isolated networks; Parshani et al. [55] studied a model more close to real systems, two partial interdependent networks, finding that the percolation transition changes from a first order to a second order at a certain critical coupling as the coupling strength decreases; Gao et al. developed an analytical framework to study the percolation of a tree-like network formed by  $n$  interdependent networks (tree-like NON) [37,78,79], discovering that while for  $n = 1$  the percolation transition is a second order, and for any  $n > 1$  where cascading failures occur, it is a first order (abrupt) transition. The tree-like NON has some other

extensions, such as the multiplex networks [73] considered as  $n$  interdependent networks without feedback condition, and the interdependent networks based on epidemic spreading [80]. More recently, Gao et al. [81] developed a general framework to study the percolation of any “network of networks”.

The process of cascading failures in network of networks is caused by the initial attack on nodes. Most of the studies above are focused on random initial failure. While in real scenarios, initial failures are mostly not random but due to targeted attack on important hubs (nodes with high degree) or occur to low degree nodes since important hubs are purposely protected [82], which triggers another branch of the studies of networks of networks. Huang et al. [82] proposed a mathematical framework for understanding the robustness of fully interdependent networks under targeted attacks, which was later extended to targeted attacks on partially interdependent networks by Dong et al. [83]. Huang et al. [82] and Dong et al. [83] developed a general technique that uses the random attack solution to map the targeted attack problem in interdependent networks. Furthermore, Dong et al. [74] extended the study of targeted attacks on high degree nodes in a pair of interdependent networks to the study of network of networks, and find that the robustness of networks of networks can be improved by protecting important hubs.

The analytic tools of the robustness of interdependent networks have been applied to various real systems, such as financial systems [84], airline systems [85], brain [86] and social systems [87], which helps us understand the catastrophic failure and crisis in complex systems in real scenarios. The applications to real systems show that the correlations between networks are common in interacting systems, and it decreases the vulnerability of the coupled systems. Parshani et al. [60] proposed an “intersimilarity” measure between the interdependent networks. They studied a system composed of the interdependent world-wide seaport and the world-wide airport networks, and found that as the interdependent networks become more intersimilar the system becomes more robust. The case in which all pairs of interdependent nodes in both networks have the same degree was solved analytically by Buldyrev et al. [88]. The effect of intersimilarity between the coupled networks on percolation was further studied analytically by Cellai et al. [89] and Hu et al. [90]. Very recently, Reis et al. [86] shows that the stability of a system of networks relies on the relation between internal structure of a network and its pattern of connections to other networks. Hu et al. [87] applied the percolation of interdependent networks with in- and out-degree correlations between two networks to coupled social networks, showing that the in- and out degree correlations between networks benefit the robustness of the coupled social systems. Thus, increasing the correlations between different coupled infrastructure systems is another method to increase the robustness of the entire systems and avoid catastrophic failures.

The studies of the vulnerability and other structural and dynamical properties of networks of networks help us understand natural and technological systems, and the ultimate proof of our understanding of them is reflected in our ability to control them [91]. Due to the large-scales and complexities, controlling complex networks still remains a huge



**Fig. 1.** (color online) Illustration of the interdependent relationship among different infrastructures [51]. These complex relationships are characterized by multiple connections between infrastructures, feed-back and feed-forward paths, and intricate, branching topologies. The connections create an intricate web that can transmit shocks throughout broad swaths of an economy and across multiple infrastructures. It is clearly impossible to adequately analyze or understand the behavior of a given infrastructure in isolation from the environment or other infrastructures. Rather, one must consider multiple interconnected infrastructures and their interdependencies. For example, the reliable operation of modern infrastructures depends on computerized control systems, from SCADA systems that control electric power grids to computerized systems that manage the flow of railcars and goods in the rail industry. In these cases, the infrastructures require information transmitted and delivered by the communication infrastructure [51]. After Ref. [52].

challenge. Liu et al. [91] have made a stepstone for the goal by studying the controllability of complex networks, and proved that the whole networks can be controlled by injecting suitable input signals to the driver nodes, whose minimum number can be determined by using the structural controllability theory. It triggers another hotspot in the research of complex networks of active pursuit [92–101]. For example, Wang et al. [102] et al. proposed a method for optimizing the controllability of complex networks by minimum structural perturbations; Jia et al. [93] discovered two distinct control modes in complex systems: centralized versus distributed control, by identifying the category of each node according to its role in control; Yan et al. [97,103] addressed the physically important issue of the energy required for achieving control; Liu et al. [100] apply the structural controllability theory to a human liver metabolic network and find that most critical driver metabolites are essential metabolites. While for large natural and technological systems, it is typically neither feasible nor necessary to control the entire network, Gao et al. [92] develop an alternative ‘*k*-walk’ theory and a greedy algorithm to study the target control of networks, and find that the structural controllability approach used for full control overestimates the minimum number of driver nodes needed for target control and many real-world networks are suitable for efficient target control. More recently, Pósfai et al. [104] have applied the controllability theory to temporal networks

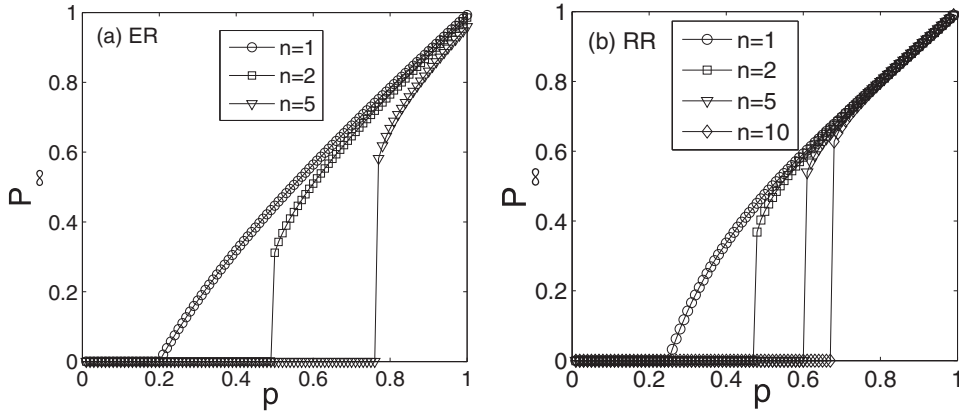
(a type of network of networks) and witnessed a phase transition describing the emergence of a giant controllable subspace. The outstanding problem of controllability of complex networks is relevant to many areas of science and engineering, and has the potential to generate technological breakthroughs as well.

## 2. Framework for a network formed of interdependent networks

Diverse networks are coupled together and depend on each other, forming a system of network of networks (NON). Understanding how the interdependence between networks affect the system robustness is one of the major challenges when designing resilient infrastructures. Here we review the theory generalization of the robustness of NON [37,78,79].

### 2.1. General framework

Consider a system (NON) composed of  $n$  nodes, where each node is a network and each link represents a *fully* or *partially* dependency relation between networks. Each network  $i$  ( $i = 1, 2, \dots, n$ ) of the NON is assumed to consist of  $N_i$  nodes linked by connectivity links, and is characterized by a degree distribution  $P_i(k)$ . Two networks  $i$  and  $j$  form a partially dependent pair if a certain fraction  $q_{ji} > 0$  of nodes of network



**Fig. 2.** Tree-like NON is composed of (a) ER networks and (b) RR networks. Plotted is  $P_\infty$  as a function of  $p$  for  $k = 5$  for RR networks composed of (a) ER and (b) RR networks for several values of  $n$ . The results obtained using Eq. (4) for ER networks, Eq. (5) for RR networks (lines), agree well with simulations (symbols). After Ref. [79].

$i$  directly depend on nodes of network  $j$ , that is, the nodes of network  $i$  will stop functioning if the nodes in network  $j$  on which they depend do not function. In each network  $i$ , we remove a fraction of  $1 - p_i$  of nodes and only a fraction nodes  $p_i$  could function after an initial attack or random failure. The assumption that only nodes that belong to the giant connected component of each network  $i$  remain functional, can be used to explain the cascade of failures: nodes in each network  $i$  that do not belong to its giant component fail, causing failures of nodes in other networks that depend on the failing nodes of network  $i$ . Such failure of the nodes in other networks will cause further failures of nodes in network  $i$  which depend on the failed nodes of the other networks, and this process will keep on iteratively until no more failure could happen. At the final steady state, the final giant component size of each network  $P_{\infty, i}$  can be computed by the equations from Ref. [81],

$$P_{\infty, i} = x_i g_i(x_i), \quad (1)$$

where  $x_i$  ( $i = 1, 2, \dots, n$ ) satisfy the following  $n$  equations,

$$x_i = p_i \prod_{j=1}^K [q_{ji} y_{ji} g_j(x_j) - q_{ji} + 1], \quad (2)$$

and the product is taken over the  $K$  networks inter-linked with network  $i$  by the partial dependency links (non-zeros  $q_{ji}$ ). If the dependencies between networks satisfy the condition of “no-feedback” (if node  $a_l$  of network  $i$  depends on node  $b_m$  of network  $j$ , and  $b_m$  depends on node  $a_n$  in network  $i$ , then  $l = n$ ) [37], the fraction of nodes in network  $j$  which survive after the damage caused by the dependencies between network  $j$  and other networks except network  $i$ , can be written as

$$y_{ij} = \frac{x_i}{q_{ji} y_{ji} g_j(x_j) - q_{ji} + 1}. \quad (3)$$

If the dependencies do not satisfy the condition of “no-feedback”, then  $y_{ij} = x_j$ .

## 2.2. Percolation laws

Next we will summarize the percolation laws in a NON for both cases where the dependencies satisfy “no-feedback” condition and where no such condition holds [37,78,79,81].

### (a) No-feedback condition

- (i) Given a tree-like NON consisting of  $n$  Erdős-Rényi (ER) [32] networks with the same average degree  $\langle k \rangle$  and each pair of networks is fully interdependent  $q_{ij} = 1$ , after removing  $1 - p$  fraction of nodes from any one of the networks, the size of the mutual giant component (the final giant components which are the same for all networks after the process of cascading failure) [78] follows,

$$P_\infty = p[1 - \exp(-\langle k \rangle P_\infty)]^n. \quad (4)$$

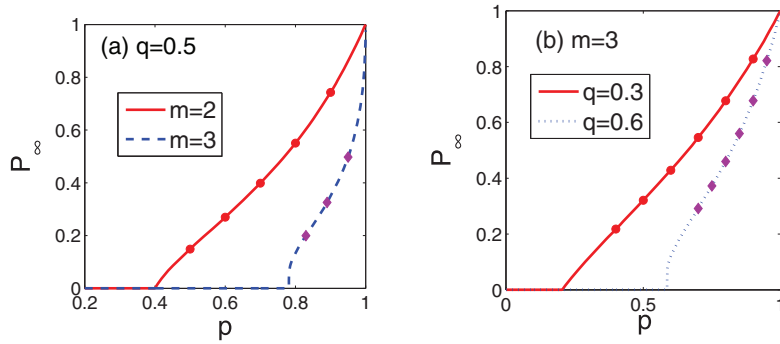
If  $n = 1$  Eq. (4) is the result for a single ER network [32] and the system shows a second order phase transition, while for  $n > 1$  the system undergoes a first order phase transition, as shown in Fig. 2(a).

- (ii) For a tree-like NON formed by  $n$  Random Regular (RR) networks [79] with the same degree  $k$ , after removing  $1 - p$  fraction of nodes from any one of the networks, the size of the mutual giant component follows:

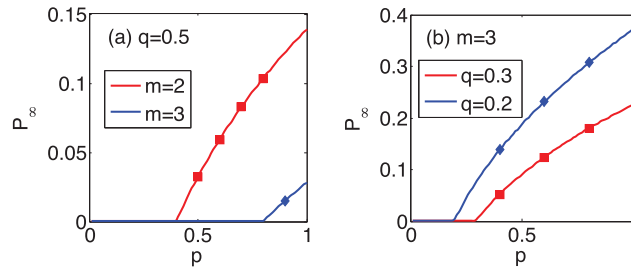
$$P_\infty = p \left\{ 1 - \left\{ p^{\frac{1}{n}} P_\infty^{\frac{n-1}{n}} \left[ \left( 1 - \left( \frac{P_\infty}{p} \right)^{\frac{1}{n}} \right)^{\frac{k-1}{k}} - 1 \right] + 1 \right\}^k \right\}^n. \quad (5)$$

If  $n = 1$ , Eq. (5) yields the result of a single RR, as shown in Fig. 2(b).

- (iii) For a NON composed by  $n$  ER network with the same average degree  $\langle k \rangle$  where each network depends on exactly  $m$  other networks (an RR network where each node is an ER network), and each pair of interdependent networks has a coupling strength  $q$ , after removing a fraction  $1 - p$  of nodes from one network, the final giant component [78] size of each network



**Fig. 3.** The giant component for an RR network composed of ER networks,  $P_\infty$ , as a function of  $p$ , for ER networks with average degree  $\langle k \rangle = 10$ . (a) for two different values of  $m$  and  $q = 0.5$ . (b) for two different values of  $q$  and  $m = 3$ . The curves in (a) and (b) are obtained using Eq. (6) and are in excellent agreement with simulations (symbols). The symbols are obtained from simulations by averaging over 20 realizations for  $N = 2 \times 10^5$ . In (a), simulation results are shown as circles ( $n = 6$ ) for  $m = 2$  and as diamonds ( $n = 12$ ) for  $m = 3$ . These simulation results support our theoretical result, Eq. (6), which is indeed independent of number of networks  $n$ . After Ref. [81].



**Fig. 4.** The giant component for an RR network of ER networks with feedback condition,  $P_\infty$ , as a function of  $p$  for ER average degree  $\langle k \rangle = 10$ , for different values of  $m$  when  $q = 0.5$  and (a) for different values of  $q$  when  $m = 3$ . The curves in (a) and (b) are obtained using Eq. (7) and are in excellent agreement with simulations (symbols). The symbols are obtained from simulations of a NON with  $n = 6$  networks forming a circle by averaging over 20 realizations with  $N = 2 \times 10^5$  with both cases  $m = 2$  and  $m = 3$ . The absence of first order regime in NON formed of ER networks is due to the fact that at the initial stage nodes in each network are interdependent on isolated nodes (or clusters) in the other network. However, if only nodes in the giant components of both networks are interdependent, all three regimes, second order, first order and collapse will occur, like in the case of RR NON formed of RR networks. After Ref. [81].

follows:

$$P_\infty = \frac{p}{2^m} (1 - e^{-(k)P_\infty}) [1 - q + \sqrt{(1 - q)^2 + 4qP_\infty}]^m, \quad (6)$$

where  $P_\infty$  does not depend anymore on the number of networks  $n$ . Note that if  $q = 0$  or  $m = 0$ , then  $P_\infty = p(1 - e^{-(k)P_\infty})$  which is again the result of a single ER network [32]. The good agreement between theory and simulations is shown in Fig. 3.

#### (b) Absence of no-feedback condition

- (iv) For a NON composed by  $n$  ER networks with the same average degree  $\langle k \rangle$  where each network depends on exactly  $m$  other networks (a RR network where each node is an ER network) and the dependencies between network do not satisfy the “no-feedback” condition. the size of the final giant component [78] for each network after removing a fraction  $1 - p$  of nodes from each network follows:

$$P_\infty = p(1 - e^{-(k)P_\infty})(1 - q + qP_\infty)^m. \quad (7)$$

- (v) For a NON composed by  $n$  RR networks with the same degree  $k$ , where each network depends on exactly  $m$  other networks (a RR network where each node is a RR network), after removing randomly a fraction  $1 - p$

of nodes from one network, the giant component [78] size of each network follows:

$$1 - \left[ 1 - \frac{P_\infty}{p(1 - q - qP_\infty)} \right]^{\frac{1}{k}} = p \left\{ 1 - \left[ 1 - \frac{P_\infty}{p(1 - q - qP_\infty)} \right]^{\frac{k-1}{k}} \right\} (1 - q + qP_\infty)^m. \quad (8)$$

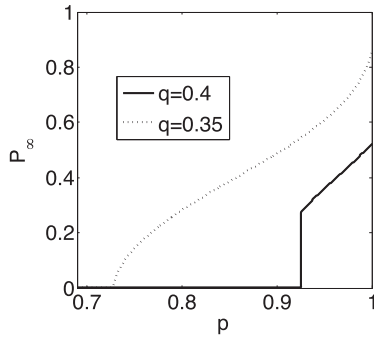
Again, both Eqs. (7) and (8), if  $m = 0$  or  $q = 0$ , show the analytical results of a single network. Eqs. (7) and (8) agree well with the simulation results, as seen in Figs. 4 and 5.

This rich generalization shows that the percolation of a single network studied for more than 50 years is a limited case of the more general case of network of networks.

#### 2.3. Robustness of network of networks under targeted attack

Most of the studies reviewed above are focused on random initial failure. While in real scenarios, initial failures are mostly not random but due to targeted attack on important hubs (nodes with high degree) or occur to low degree nodes since important hubs are purposely protected [82]. For example, on one hand, hackers usually attack the highly connected





**Fig. 5.** The giant component for an RR NON formed of RR networks with feedback condition,  $p_\infty$ , as a function of  $p$  for RR of degree  $k = 6$  and  $m = 3$ , for two different values of  $q$ . The curves are obtained using Eq. (8), which shows a first order phase transition when  $q$  is large but a second order phase transition when  $q$  is small. After Ref. [81].

computers so as to breakdown a computer network, and on the other hand, heavily connected hubs in an internet network are purposely more secured; in a social network, members of a group that have more links to others have a lower probability to leave the group [8]. Especially, most networks in real world are resilient to random removal of nodes but sensitive to intentional attack [105]. Accordingly, the system of a network of networks may show different properties under random failures and targeted attacks.

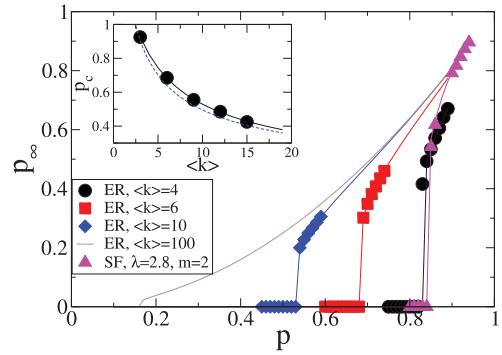
Huang et al. [82] studied the robustness of interdependent networks under an initial targeted attack, where the probability to attack a node depends on the degree of the nodes. Each node in interdependent networks is assigned with a probability  $W_\alpha(k_i)$  that a node  $i$  with  $k_i$  links is initially removed, whose function is

$$W_\alpha(k_i) = \frac{(k_i + 1)^\alpha}{\sum_{i=1}^N (k_i + 1)^\alpha}, \quad -\infty < \alpha < +\infty, \quad (9)$$

where the parameter  $\alpha$  characterizes the vulnerability of each node. When  $\alpha > 0$ , nodes with a higher degree are more vulnerable for the intentional attack, while for  $\alpha < 0$ , nodes with a higher degree are defended and so have lower probability to fail. The case  $\alpha = 0$ ,  $W_0 = 1/N$ , is equivalent to random removal of nodes [54,55]. An important special case  $\alpha = 1$  corresponds to the acquaintance immunization strategy [106] and can be solved analytically. By mapping the targeted-attack problem in interdependent networks to the random-attack problem in a transformed pair of interdependent networks and using the generating function, Huang et al. [82] develop an analytic framework to solve the robustness of interdependent networks under targeted attack. When  $\alpha = 1$ , the size of the final giant component of interdependent ER networks  $p_\infty$  can be explicitly solved by

$$p_\infty = p^2 (1 - e^{-(k)t^2 p_\infty})^2, \quad (10)$$

where  $t = \frac{\ln(p)}{\langle k \rangle} + 1$ . As shown in Fig. 6, the targeted attack increases the percolation threshold  $p_c$ , which means interdependent networks become more vulnerable. The models studied in this work [82] are fully interdependent networks. Dong et al. have extended the study to partially interdependent networks [83] and network of networks [74] and find that a network of networks becomes significantly more vulnerable



**Fig. 6.** Values of  $p_\infty$  vs  $p$  when both networks are initially attacked. Both networks in the interdependent networks are ER or SF networks with the same average degree. The symbols represent simulation data ( $N = 10^6$  nodes). The solid lines are theoretical predictions, Eq. (10). The dashed line represents simulation data for interdependent scale-free networks with  $\lambda = 2.8$ ,  $\langle k \rangle = 4$ . All results are for  $\alpha = 1$ . Inset: Values of  $p_c$  vs average degree of ER networks. The symbols represent simulation data, while the line is the theory. After Ref. [82].

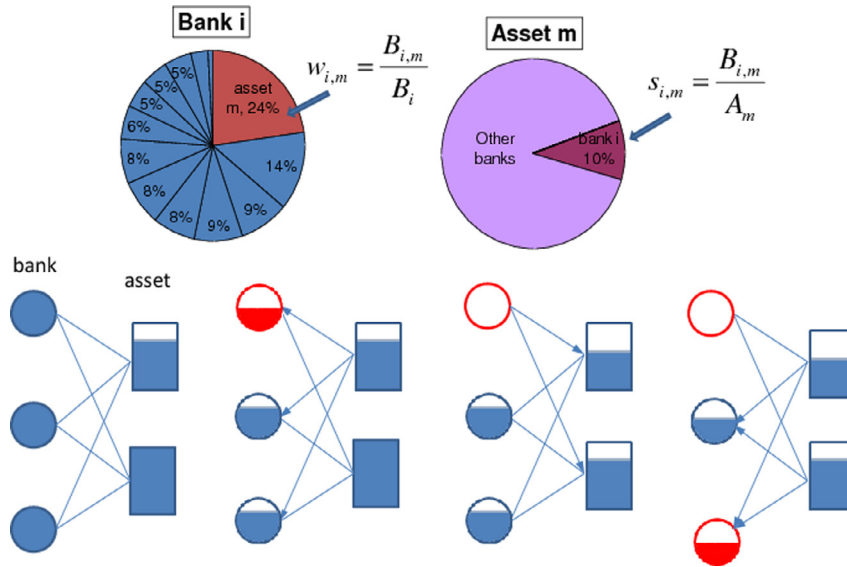
when  $\alpha > 0$  nodes with higher degrees have higher probability to fail.

### 3. Percolation of real networks of networks

The 28 September 2003 electrical blackout in Italy resulted in a widespread failure of the railway network, health-care systems, and financial services and, in addition, severely influenced communication networks. The partial failure of the communication system in turn further impaired the power grid management system, thus producing a negative feedback on the power grid [107]. Such interdependence between the power grid and communication networks triggers the development of the interdependent networks model [54] and many follow-up studies. The analytic tools of the robustness of interdependent networks also have been applied to various real systems, such as financial systems [84], airline systems [85], brain systems [86] and social systems [87], which helps us understand the catastrophic failure and crisis in complex systems in real scenarios.

#### 3.1. Application to coupled financial and economic systems

Economic and financial systems, such as real estate markets and banking systems, become increasingly interconnected and depend on each other, leading to the fact that a shock in a financial network can provoke significant cascading failures throughout the global economic system, especially, if the shocked nodes are hubs or are highly central in the network. For example, the current EU sovereign debt crisis and the 2008 world financial crisis are global cascading failure in economic systems caused by the local exogenous or endogenous shocks [84,107]. In financial systems, banks are among the most important entities, the risk spreads in which mainly via two channels: (i) direct inter-bank liability linkages between financial institutions, which has been given extensive empirical and theoretical studies [108–110], focusing on the dynamics of loss propagation via the complex network of direct counterpart exposures following an



**Fig. 7.** Bank-asset bipartite network model with banks as one node type and assets as the other node type. Link between a bank and an asset exists if the bank has the asset on its balance sheet. Upper panel: illustration of bank-node and asset-node.  $B_{i,m}$  is the amount of asset  $m$  that bank  $i$  owns. Thus, a bank  $i$  with total asset value  $B_i$  has  $w_{i,m}$  fraction of its total asset value in asset  $m$ .  $s_{i,m}$  is the fraction of asset  $m$  that the bank holds out. Lower panel: illustration of the cascading failure process. The rectangles represent the assets and the circles represent the banks. From left to right, initially, an asset suffers loss in value which causes all the related banks total assets to shrink. When a banks remaining asset value is below certain threshold (e.g. the banks total liability), the bank fails. Failure of the bank elicits disposal of bank assets which further affects the market value of the assets. This adversely affects other banks that hold this asset and the total value of their assets may drop below the threshold which may result in further bank failures. This cascading failure process propagates back and forth between banks and assets until no more banks fail. After Ref.[84].

initial default. (ii) contagion via changes in bank asset values, based on bank financial statements and financial ratio analysis, which has received scant attention. A financial shock that contributes to the bankruptcy of a bank in a complex network will cause the bank to sell its assets. If ability of the market to absorb these sales is less than perfect, the market prices of the assets that the bankrupted bank sells will decrease. Other banks that own similar assets could also fail because of loss in asset value and increased inability to meet liability obligations. This imposes further downward pressure on asset values and contributes to further asset devaluation in the market. Damage in the banking network thus continues to spread, and the result is a cascading of risk propagation throughout the system [84,111].

Between 2000 and 2007, 27 banks failed in the US, but between 2008 and early 2013 the number rose to over 470. The names of the failed banks and the time when they failed were recorded by Federal Deposit Insurance Corporation (FDIC). By analyzing the properties of the failed banks from FBL-FDIC, examining the weights in specific assets as well as equity to asset ratios, Huang et al. [84] construct a bipartite banking network that is composed of two types of nodes, (i) banks and (ii) bank assets. Link between a bank and a bank asset exists when the bank has the asset on its balance sheet, as shown in Fig. 7. They also develop a cascading failure model capturing the effect of the 2008 real estate market failure on the US banking network. Populating the model by the banks balance sheet data (CBBSD) for 2007, and running the cascading failure model by initially introducing a shock to the banking system, they find that the model simulates well the

crisis spreading process and identifies a significant portion of the actual failed banks, by comparing the failed banks identified by model with the actual failed banks from the FBL-FDIC from 2008 to 2011. This coupled bank-asset network model can be used to study the cascading failure of banks step by step, characterizing the spreading of financial crisis, which indicates that this model is useful for systemic risk stress testing for financial systems. For example, the model can be stress tested to predict which banks could be in danger and how many banks could fail if the agricultural assets drop 20% in value, based on which, policy suggestions such as requirement to reduce exposure to agricultural loans or closely monitor vulnerable banks could be proposed. The risk in the banking system propagates bidirectionally between assets and banks. Suppressing propagation either way could be very helpful to mitigating such catastrophes. The first way is to provide liquidity to the market, thus when distressed banks need to sell assets, the market will not overreact. The second way to curb systemic risk contagion is to ensure that banks are solvent and have healthy balance sheets, i.e. no excess leverage, higher capital requirements, appropriate levels of liquid assets, etc. in order to be able to absorb shocks to the asset value. The model shows that sharp transitions can occur in the coupled bank-asset system and that the network can switch between two distinct regions, stable and unstable, which means that the banking system can either survive and be healthy or collapse. The model also identifies that commercial rather than residential real estate assets are major culprits for the failure of over 350 US commercial banks during 2008 to 2011.

### 3.2. Application to other real interdependent networks

Brain and cellular networks are organized in interconnected networks. The connectivity and interdependence between networks largely decrease the robustness of systems, leading to the fact that abrupt failures easily show up in systems. Very recently, Reis et al. [86] shows that the stability of a system of networks relies on the relation between internal structure of a network and its pattern of connections to other networks. A theory has been developed for the systems of structured networks, identifying a structural communication protocol that ensures the system of networks is stable (less susceptible to catastrophic failure) and optimized for the fast communication across the entire system [86]. The theory establishes concrete predictions of a regime of correlated connectivity between networks composing the system. The predictions have been tested by two different systems of brain connectivity based on functional magnetic resonance imaging (fMRI) data. The brain organizes in a series of interacting networks [112], presenting a paradigmatic case study for a theory of connected correlated networks. For two independent experiments of functional networks in task and resting states in humans, the systems of brain networks organize optimally, as predicted by the theory. Such understanding of the interconnected natural systems, for example, brain networks, could provide ways to increase the robustness of the man-made systems, e.g. increasing the correlations between different coupled infrastructure systems could increase the robustness of the entire systems and avoid catastrophic failures.

Moreover, the percolation theory of interdependent networks have been applied to many other real coupled systems and uncovering many interesting and useful results. For example, Hu et al. [87] applied the percolation of interdependent networks with in- and out- degree correlations between two networks to coupled social networks, showing that the in- and out degree correlations between networks benefit the robustness of the coupled social systems. Radicchi et al. [85] introduced a theory to fully characterize percolation phase diagrams in finite-size interdependent networks, identifying cores of quality links able to prevent catastrophic failures in real systems. For example, the *H. sapiens* protein interaction network and the *C. elegans* connectome undergo smooth percolation transitions, and the multi-layer air transportation networks within the US shows a small discontinuity, whose height of jump is not as marked as observed as in random uncorrelated networks. The quality links mainly correspond to hub-to-hub links, and it could increase the systems robustness.

## 4. Controllability of networks of networks

In the past decade, plenty of attention has been poured into the study of the structure and dynamics of complex networked systems [54,113–115]. One final goal of our effort for understanding complex networks is to control the complex systems in our daily life. Due to the large-scales and complexities, controlling complex networks still remains a huge challenge. Liu et al. [91] have strived a big step towards the goal by studying the controllability of complex networks, triggering another hotspot in the research of complex networks

[92–101]. More recently, Pósfai et al. [104] and Pan et al. [116] have applied the controllability theory to temporal networks (a type of network of networks), and the structural controllability theory has been applied to multiplex networks [117–120]. The outstanding problem of controllability of complex networks is relevant to many areas of science and engineering, and has the potential to generate technological breakthroughs as well.

### 4.1. Controllability of complex networks

A dynamic system is controllable indicating that with a suitable choice of inputs, it can be driven from any initial state to any desired final state within a finite time interval [121]. Before the work of Liu et al. [91], fundamental questions pertaining to the controllability of complex systems emerging in nature and engineering have resisted advances, due to the fact that two independent factors contribute to controllability, each with its own layer of unknown: (1) the systems architecture, represented by the network encapsulating which components interact with each other; and (2) the dynamical rules that capture the time-dependent interactions between the components. With the advance towards quantifying the topological characteristics of complex networks, Liu et al. [91] introduced an analytical framework to study the controllability of complex networks via a combination of tools from network science, control theory and statistical physics.

The dynamics of most real systems is driven by nonlinear processes. However, the dynamical rules of real-world networks are so diverse that writing a general dynamical equation that captures them all is plainly impossible. Moreover, for many networks, especially biological networks, we do not even know the dynamical rules. Thus, before we explore the fully nonlinear dynamical problem, we have to understand the impact of the topological characteristics on linear control, which naturally serves as a prerequisite of the nonlinear controllability problem. Furthermore, the controllability of nonlinear systems is often structurally similar to and determined by the systems linearized dynamics [122]. Indeed, a basic starting point for exploring the controllability of any nonlinear system is the study of the linearized version of the nonlinear dynamical system. Therefore, we start with the canonical linear time-invariant dynamics [11].

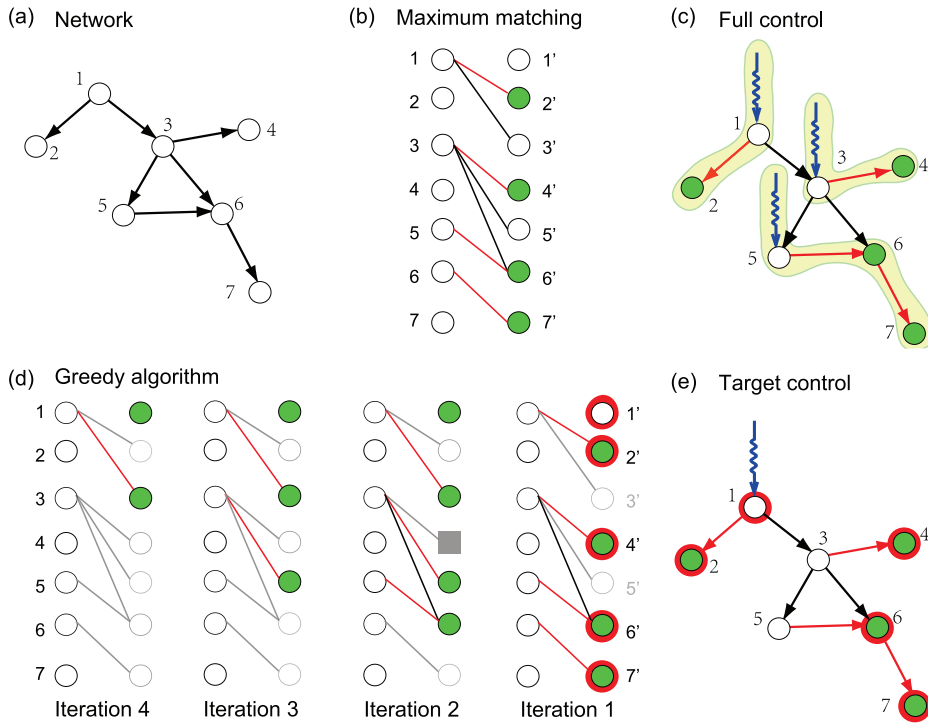
$$\frac{dx(t)}{dt} = Ax(t) + Bu(t), \quad (11)$$

where the vector  $x(t) = (x_1(t), x_2(t), \dots, x_N(t))^T$  describes the state of a system of  $N$  nodes at time  $t$ . The  $N \times N$  matrix  $A$  is the transpose of the adjacency matrix which captures the systems wiring diagram and the interaction strength between individuals. The  $N \times M$  matrix  $B$  is the input matrix ( $N \geq M$ ), which identifies the nodes where the input signals are injected.  $M$  characters the number of input signals. The input vector is denoted by  $u(t) = (u_1(t), u_2(t), \dots, u_M(t))^T$ . According to Kalman's controllability rank condition [121], the system represented by Eq. 11 is controllable if and only if the  $N \times NM$  controllability matrix  $C$  has full rank, i.e.,

$$\text{rank}(C) = \text{rank}[B, AB, A^2B, \dots, A^{N-1}B] = N. \quad (12)$$

This controllability rank condition indicates that in order to control the full network, it is needed to identify the





**Fig. 8.** Controlling a small network. (a) A directed network with seven nodes. (b) Maximum matching of the network in its bipartite representation. Matching edges are shown in red, matched nodes  $\{x_2, x_4, x_6, x_7\}$  are green and unmatched nodes  $\{x_1, x_3, x_5\}$  are white. (c) By controlling the three unmatched nodes (driver nodes) and ensuring that there are no inaccessible nodes, the system is guaranteed to be structurally controllable. (d) Greedy algorithm developed for target control. Here the target set is  $\{x_1, x_2, x_4, x_6, x_7\}$  (highlighted in red). In the first iteration, we match all target nodes by solving a maximum matching problem on an induced bipartite graph. Target nodes  $\{x_2, x_4, x_6, x_7\}$  (in green) are matched by  $\{x_1, x_3, x_5, x_6\}$ , which are the new target nodes considered in iteration 2. After four iterations, we obtain that node  $x_1$  is the driver node for the target set  $\{x_1, x_2, x_4, x_6, x_7\}$ . (e) By controlling the unmatched node  $x_1$  calculated from the GA, the target set  $\{x_1, x_2, x_4, x_6, x_7\}$  is guaranteed to be controllable. The red lines are the matched links obtained in the first iteration of greedy algorithm. After Ref. [92] (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article).

number of signals, and the nodes where the signals are injected, called driver nodes. By injecting different input signals to each node of the minimum set of driver nodes, the whole network can be sufficiently controlled. However it is practically difficult to check this condition for many real networks such as biological, technological and social systems due to their complexity and the unknown of the weight of each link. As the number of input combinations grows exponentially with the number of nodes ( $\sim 2^N$ ), which is a computationally prohibitive task for large networks. To overcome these two difficulties, Liu et al. [91] studied the structural controllability of complex networks. A system  $(A, B)$  is structurally controllable, indicating that it is possible to choose a combination of non-zero weights in  $A$  and  $B$  such that the system satisfies Eq. 12. Usually, a structurally controllable system are controllable for almost all weight combinations, except for some pathological cases [123], thus structural controllability implies controllability of a continuum of linearized systems [124], providing a sufficient condition for controllability for most nonlinear systems. To avoid the brute-force search for driver nodes, the structural controllability problem [123] can be mapped into a maximum matching problem [125]. The maximum matching is the maximum set of links that do not share start or end nodes as shown in Fig. 8. A node is said to be matched if a link in the maximum matching points at it; otherwise it is unmatched. If the nodes

in a network are all matched, then the network is perfectly matched and the minimum number of driver nodes  $N_D$  is 1; otherwise  $N_D = N - N_M$ , where  $N_M$  is the number of matched nodes. The minimum number of driver nodes is determined by the network's degree distribution and it is higher in sparse inhomogeneous networks than that in dense and homogeneous networks. Counterintuitively, in both model and real systems, the driver nodes tend to avoid high-degree nodes.

Since then, the driver nodes and their number  $N_D$  characterizing the controllability of complex networks, capture plenty attention from the scientists in the field of network science. For example, Wang et al. [102] proposed a method to optimize the controllability of complex networks by minimum structural perturbations; Yan et al. [97,103] addressed the physically important issue of the energy required for achieving control by deriving and validating scaling laws for the lower and upper energy bounds; Liu et al. [126] introduced the concept of control centrality to quantify the ability of a single node to control a directed weighted network; Jia et al. [93] discovered two distinct control modes in complex systems: centralized versus distributed control, by identifying the category of each node; Liu et al. [101] apply the structural controllability theory to a human signaling network and find that inputting different control signals on the regulators of the cancer-associated genes could cost less than controlling the cancer-associated genes directly in order to control

the whole human signaling network in the sense that less drive nodes are needed.

#### 4.2. Target control of complex networks

The minimum set of driver nodes identified by Liu et al. [91] are sufficient to control the whole network. For engineered systems, such as the auto-pilot system of an airplane, full control is essential. However, many biological, technological and social systems are massive in size and complexity, hence it is neither feasible nor necessary to control the entire network. Instead, it is more realistic and sufficient to achieve target control, that is, to control a subset of target nodes (or a subsystem) that are essential for the system's mission pertaining to a selected task. Recently, Gao et al. [92] study the target control of complex networks and find that the structural controllability approach used for full control overestimates the minimum number of driver nodes needed for target control. Given a system with the canonical linear time-invariant dynamics [92]

$$\begin{cases} \dot{x} = Ax + Bu, \\ y = Cx, \end{cases} \quad (13)$$

where  $x$ ,  $A$ ,  $B$  and  $u$  are the same as those in Eq. 11, and  $y \in \mathbb{R}^S$  and  $C \in \mathbb{R}^{S \times N}$  represent the output vector and output matrix, identifying the target nodes we want to control. The system  $(A, B, C)$  is said to be target controllable with respect to a given target node set  $C$  if there exist a time-dependent input vector  $u(t) = (u_1(t), u_2(t), \dots, u_M(t))^T$  that can drive the state of the target nodes to any desired final state in finite time. The system  $(A, B, C)$  is target controllable if and only if the dimension of the output controllable subspace  $d(A, B, C)$  satisfies

$$d(A, B, C) = \text{rank}[CB, CAB, CA^2B, \dots, CA^{N-1}B] = S. \quad (14)$$

To solve the target control problem in the single-input case, a new approach was developed [92] called the ‘ $k$ -walk’ theory, based on the principle that a node can control a target set of nodes provided that the length of the path from the control node to each target node in the set is unique. Using the  $k$ -walk theory, all sets of nodes that can be controlled by the given node can be identified, and it has been rigorously proved that the  $k$ -walk theory is correct for directed tree-like networks, that is, networks with no loops. However, the  $k$ -walk theory is only applicable for the single-input case. For networks requiring more than one control input, the authors develop a greedy algorithm (GA) that offers a good approximation to the minimum set of inputs sufficient for target control, as shown in Fig. 8. Both the  $k$ -walk theory and the GA are based on the structural control theory [91,123], that is, the system parameters are either fixed at zero or are independent free parameters. The minimum number of driver nodes for full control yields an upper bound of the minimum number  $P_D$  for target control (denoted with  $P_D^{UB}$ ). The lower bound of  $P_D$ , denoted with  $P_D^{LB}$ , can also be obtained using maximum matching. The maximum matching in a bipartite graph connecting on one side (1) the target nodes ( $C$  nodes), and on the other (2) the nodes that can reach the target nodes via (3) the edges among them. If a target node is unmatched, we must drive it directly, and the number of unmatched target nodes is the lower bound of  $P_D$ . As shown in Fig. 8, the

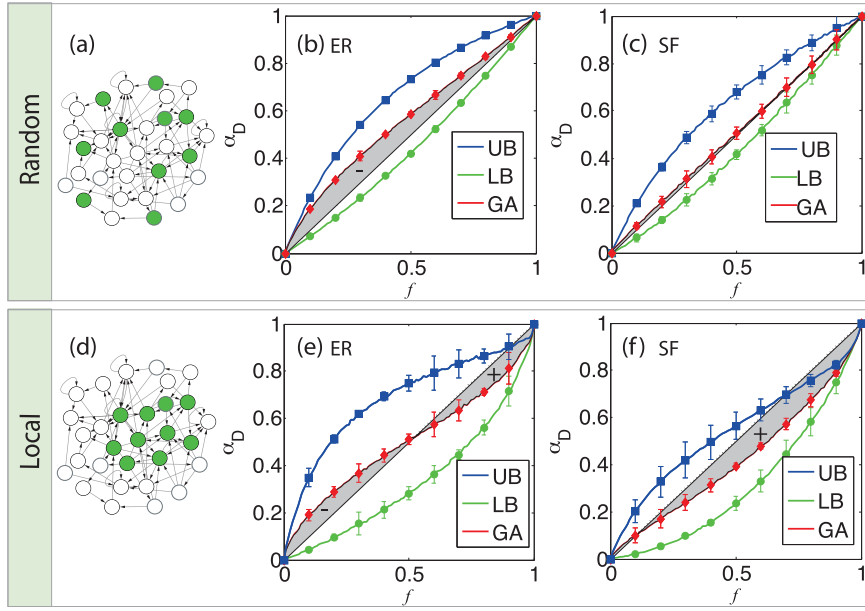
lower bound of  $P_D$  is given by the first iteration of the GA, that is,  $P_D^{LB} = 1$  for the target nodes 1, 2, 4, 6, 7, because in the first iteration only node 1 is unmatched.

In Ref. [92] Gao et al. study two distinct schemes for choosing the subset of nodes to control. In the random scheme, a fraction  $f$  of nodes are chosen uniformly at random. In the local scheme, the chosen nodes form a connected component, capturing a well-defined local network neighbourhood. To develop an efficiency measure of target control, they compared  $P_D$ , which is the minimum number of driver nodes needed to control the fraction  $f$  of target nodes, with  $fN_D$ , which is the corresponding relative fraction of the driver nodes needed for full control. If  $P_D$  is less than  $fN_D$  then target control is more efficient than full control for a given  $f$ . The authors also establish the overall target control efficiency by considering the integrated efficiency across the entire range of  $0 < f \leq 1$ . For both SF and ER networks, in general, local target control is more efficient than random target control, as shown in Fig. 9. More surprisingly, the degree heterogeneous networks, such as SF networks, have higher specific and overall target control efficiency than degree homogeneous networks (Fig. 9), for both random and local schemes, when the average degree of the network is large. In contrast, for full control, degree homogeneous networks, such as ER networks, are more efficient than the corresponding degree heterogeneous networks [91]. Finally, the methods have been applied to real data, confirming that many real-world networks display high efficiency of target control.

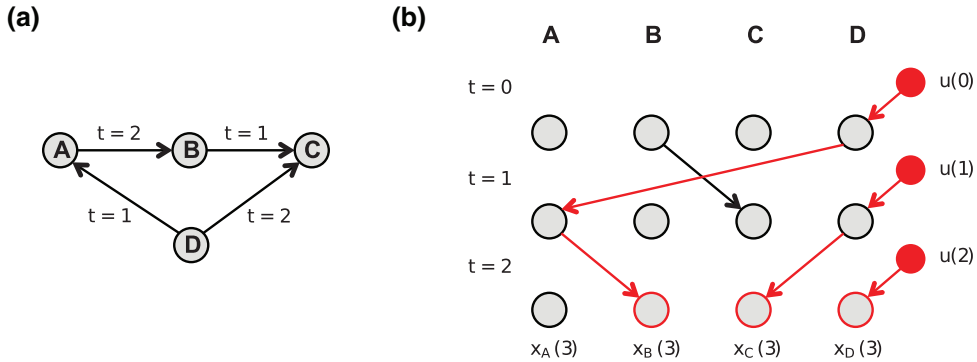
#### 4.3. Structural controllability of temporal networks

The structures of some complex systems are usually not static but dynamically changing with time, and such systems can be modeled as temporal networks, e.g., the topology of telephone communication networks [127], international trade networks [128] and transportation networks [43] are all different among different time period. It is necessary to take into account temporal information of the connections when the interaction events are not evenly distributed over time, but have nontrivial temporal correlations [129,130]. The temporal sequence of interactions governs information spreading processes [104], and the way that information spreads among networks largely influence their controllability. For example, a small communication network of three individuals  $A$ ,  $B$  and  $C$  (Fig. 10). Assume that  $B$  sends an email to  $C$  at time  $t = 1$ , and  $A$  sends an email to  $B$  at time  $t = 2$ . Neglecting the temporal sequence, we find that information may spread from  $A$  to  $C$ . However, taking the order of the messages into account, this is obviously not possible, which has a clear consequence for control: we cannot influence  $C$  using  $A$ . Therefore, one must include the temporal aspect of the interactions when studying the controllability of networks with time-varying topology. In general, a temporal network can be considered as a tree-like network.

Pósfai et al. [104] provided analytic and computational tools to study controllability based on temporal network characteristics. The system studied in this work consists of a temporal sequence of directed networks and the network topology of these networks are comparable. All these temporal networks can be denoted by a general network formalism by assigning a time stamp  $t$  to each link. The temporal



**Fig. 9.** Random versus local target controllability of two canonical network models. (a), (b) and (c) Random selection scheme. (a) Illustrating random selection of  $f = 1/3$  target nodes. (b) For ER networks with average degree  $\langle k \rangle = 5.6$ , we show the normalized fraction of driver nodes ( $\alpha_D$ ) in function of the target node fraction  $f$  for the random selection scheme. (c) For SF networks with  $\langle k \rangle = 5.6$  and exponent  $\lambda = 2.4$ , we show the normalized fraction of driver nodes ( $\alpha_D$ ) as a function of the target node fraction  $f$  for the random scheme. (d), (e) and (f) Local selection scheme. (d) The selection of an  $f = 1/3$  target node with the local scheme. (e) ER networks with the same average degree as in (b). (f) SF networks with the same  $\langle k \rangle$  and  $\lambda$  as in (c). In each figure, we denote UB as the upper bound, GA as the greedy algorithm and LB as the lower bound of the minimum number of driver nodes to control an  $f$  fraction of target nodes. For ER networks, random target control is always less efficient than the full control, and for local target control efficiency depends on  $f$ . For SF networks random target control is as efficient as full control, but significant gains in efficiency are observed for local target control. Furthermore, for ER and SF networks local target control is more efficient than random target control. After Ref.[92].



**Fig. 10.** Controlling a simple temporal network. (a) In the aggregated network, information can spread from node A to C, however, it is forbidden if the temporal order of the interactions is taken into account. As a consequence, we cannot control C by imposing a control signal on A. (b) We visualize the dynamics represented by the small temporal network by creating a copy of each node for each time step. The state of the node in the layer  $t + 1$  is determined by its neighbors in layer  $t$ . We aim to control the system at  $t = 3$  in  $\Delta t = 3$  time steps. We use D as an input node, meaning that we can intervene at D in layers  $t = 1, 2, 3$ . According to the independent path theorem, we can control the nodes in layer  $t = 3$  that can be connected to intervention points via independent paths, therefore we control nodes B, C and D. After Ref.[104].

networks are composed of a set of nodes  $V = \{v_1, v_2, \dots, v_N\}$  and a set of temporal links  $E = \{e_1, e_2, \dots, e_L\}$ . Each temporal link  $e = (v_i, v_j, \omega_{ij}, t) \in E$  represents that there is information flow from node  $v_i$  to node  $v_j$  at time  $t$ , and  $\omega_{ij}$  is the weight describing the strength of the interaction between node  $v_i$  and node  $v_j$ . In each time step  $t$ , the temporal network can be regarded as a discrete time-varying linear dynamical system

$$x(t+1) = A(t)x(t) + B(t)u(t), \quad (15)$$

where the vector  $x(t) \in \mathbb{R}^N$  represents the state variables,  $x_i(t)$  corresponding to the state of node  $v_i$  at time  $t$ . The first term describes the internal dynamics of the system, the matrix  $A(t) \in \mathbb{R}^{N \times N}$  is the transpose of the weighted adjacency matrix at time  $t$ . The second term describes the control applied to the system: if we impose an outside signal on node  $v_i$  at time  $t$  changing the state of the node at time  $t + 1$ , we say that we intervene at node  $v_i$ , and we call the  $(v_i, t + 1)$  pair an intervention point. The vector  $u(t) \in \mathbb{R}^{N(t)}$  is a list of

interventions, where  $N_i(t)$  is the number of interventions at time  $t$ . The nonzero elements of matrix  $\mathbf{B}(t) \in \mathbb{R}^{N \times N_i(t)}$  identify the intervention points.

A subset of nodes  $C \subseteq V$  is called a structural controllable subspace at target time  $t$  in  $\Delta t$  time steps, if the state of all nodes  $v \in C$  can be driven from any initial state to any final state at time  $t$ , in at most  $\Delta t$  time steps by appropriately choosing  $u(t)$ . Pósfai et al. [104] prove a independent path theorem that  $C$  is a structurally controllable subspace, if all nodes  $v \in C$  at time  $t$  are connected to intervention points through independent time-respecting paths of length of at most  $\Delta t - 1$ . A time-respecting path is a sequence of adjacent temporal links such that subsequent links in the path are active in subsequent time steps, e.g. the link  $(v_i, v_j, t)$  may be followed by  $(v_j, v_k, t + 1)$ . Two paths are independent if they do not pass the same node at the same time. They also use the Ford–Fulkerson algorithm to detect the maximum controllable subspace  $N_C(v, t, \Delta t)$  using a single input node  $v$ . The controllability of a temporal network can be characterized as the average maximum controllable subspace

$$N_C(t, \Delta t) = \frac{1}{N} \sum_{v \in V} N_C(v, t, \Delta t). \quad (16)$$

For a generic class of temporal network models, a phase transition appears describing the sudden emergence of a giant controllable subspace spanning a finite fraction of the network. Moreover, the overall activity and the degree distribution of the underlying network are the main features influencing controllability.

## 5. Conclusion

We have reviewed recent studies on the vulnerability and controllability of networks of networks. It is increasingly clear that most real-world systems are not isolated but interact with each other. Studies on single networks are not enough to explain some phenomena such as species extinction and power grid blackout, and this are caused by the interactions between different systems, which can be modeled as a network of networks. In a network of networks, when a node in one network fails, it usually causes dependent nodes in other networks to fail, which, in turn, may cause further damage in the first network and result in a cascade of failures with sometimes catastrophic consequences. For the dynamics of the cascading failures and in particular how they behave with time (number of steps) see Zhou et al. [131]. The analytic framework of the percolation of network of networks represents a general result that includes as a specific case of percolation of a single network [78]. Moreover, the analytic tools of the robustness of interdependent networks have been applied to various real systems. The interdependence between networks can be used to explain the world financial crisis, which are global cascading failure in economic systems caused by the local exogenous or endogenous shocks [84]. In real scenarios, there exist correlations between coupled networks and the degree correlations between different networks are found to decrease the system's vulnerability [85–87]. The studies of networks of networks help us understand the vulnerability of interdependent systems and discover methods for improving the system's robustness. For example, the study of the robustness of networks of networks

under targeted attack find that the robustness of coupled systems can be improved by protecting the hubs [74,82], and system's robustness can be improved by designing dependency links such that they connect the nodes with similar degrees [86].

We also reviewed the studies on the controllability of isolated networks and temporal networks. They showed that the whole networks can be controlled by injecting suitable input signals to the driver nodes, and the minimum number of driver nodes can be determined by using the structural controllability theory. While for large natural and technological systems, it is typically neither feasible nor necessary to control the entire network, Gao et al. [92] develop an alternative 'k-walk' theory and a greedy algorithm to study the target control of networks, and find that the structural controllability approach used for full control overestimates the minimum number of driver nodes needed for target control and many real-world networks are suitable for efficient target control. Moreover, we review the work by Pósfai et al. [104], they have applied the structural controllability theory to temporal networks (a type of network of networks) and witnessed a phase transition describing the emergence of a giant controllable subspace.

The study of the vulnerability and controllability of networks of networks has attracted many attentions from scientists and many interesting results have been uncovered, but there are still many challenges in front of us. The applications of the percolation theory to real-world interdependent systems are based on certain assumptions, it is still challenging to develop mathematical tools for studying models based on data of real-world interdependent systems. How to control large complex networks remains to be a huge challenge, and the temporal networks studied in Ref. [104] is a limited special case of network of networks. Another challenge is to study the controllability of a general network of networks.

## Acknowledgments

We acknowledge the support from the US Army Research Laboratory and the US Army Research Office under Cooperative Agreement W911NF-09-2-0053, MULTIPLEX (EU FP7 317532), and the John Templeton Foundation ID #PFI-777, as well as the Defense Threat Reduction Agency Basic Research Grant No. HDTRA1-10-1-0100/BRBAA08-Per4-C-2-0033. We also thank Chinese Natural Science Foundation (61374160 and 61370105) for support. XL thanks the financial support for this work from the Fundamental Research Funds for the Central Universities (HUST2013TS124) and Natural Science Foundation of Hubei Province (Grant No. 2013CFB159). HP thanks the support from Zhejiang Provincial Natural Science Foundation of China (Grant No. LQ13F020007) and Shanghai Information Security Key Laboratory of Integrated Management of Technology (Grant No. AGK2013003).

## References

- [1] Watts DJ, Strogatz SH. Collective dynamics of 'small-world' networks. *Nature* 1998;393:440–2.
- [2] Barabási A-L, Albert R. Emergence of scaling in random networks. *Science* 1999;286(5439):509–12.
- [3] Albert R, Jeong H, Barabási A-L. Error and attack tolerance of complex networks. *Nature* 2000;406(6794):378–82.



- [4] Cohen R, Erez K, Ben-Avraham D, Havlin S. Resilience of the internet to random breakdowns. *Phys Rev Lett* 2000;85(21):4626.
- [5] Callaway DS, Newman ME, Strogatz SH, Watts DJ. Network robustness and fragility: percolation on random graphs. *Phys Rev Lett* 2000;85:5468.
- [6] Albert R, Barabási A-L. Statistical mechanics of complex networks. *Rev Modern Phys* 2002;74(1):47–97.
- [7] Barrat A, Barthélemy M, Pastor-Satorras R, Vespignani A. The architecture of complex weighted networks. *Proc Natl Acad Sci* 2004;101(11):3747–52.
- [8] Gallos LK, Cohen R, Argyrakis P, Bunde A, Havlin S. Stability and topology of scale-free networks under attack and defense strategies. *Phys Rev Lett* 2005;94(1):188701.
- [9] Song C, Havlin S, Makse HA. Self-similarity of complex networks. *Nature* 2005;433(7024):392–5.
- [10] Newman M, Barabási A-L, Watts DJ. The structure and dynamics of networks. Princeton University Press; 2006.
- [11] Cohen R, Havlin S. Complex networks: structure, stability and function. Cambridge University Press; 2009.
- [12] Daqing L, Kosmidis K, Bunde A, Havlin S. Dimension of spatially embedded networks. *Nat Phys* 2011;7(6):481–4.
- [13] Newman MEJ. Networks: an introduction. New York: Oxford University Press; 2010.
- [14] Dorogovtsev SN, Mendes JF. Evolution of networks: from biological nets to the internet and WWW (Physics). New York: Oxford University Press; 2003.
- [15] Satorras A, Vespignani RP. Evolution and structure of the internet: a statistical physics approach. Cambridge: Cambridge University Press; 2004.
- [16] Caldarelli A, Vespignani G. Large scale structure and dynamics of complex webs. New York: World Scientific; 2007.
- [17] Barrat A, Marc Barthélemy, and Alessandro Vespignani. Dynamical Processes on Complex Networks. Cambridge: Cambridge University Press; 2008.
- [18] Barthélemy M. Spatial networks. *Phys Rep* 2011;499:1–101.
- [19] Strogatz SH. Exploring complex networks. *Nature* 2001;410:268–76.
- [20] Bashan A, Bartsch RP, Kantelhardt JW, Havlin S, Ivanov PC. Network physiology reveals relations between network topology and physiological function. *Nat Commun* 2012;3:702.
- [21] Ludescher J, Gozolchiani A, Bogachev MI, Bunde A, Havlin S, Schellnhuber HJ. Improved el niño forecasting by cooperativity detection. *Proc Natl Acad Sci* 2013;110(29):11742–5.
- [22] Faloutsos M, Faloutsos P, Faloutsos C. On power-law relationships of the internet topology. *ACM SIGCOMM Computer Communication Review*, 29. Massachusetts: ACM.; 1999. p. 251–62.
- [23] Handcock MS, Raftery AE, Tantrum JM. Model-based clustering for social networks. *J R Stat Soc: Ser A (Stat Soc)* 2007;170(2):301–54.
- [24] Jackson MO, Rogers BW. Meeting strangers and friends of friends: how random are social networks? *Am Econ Rev* 2007;97:890–915.
- [25] Borgatti SP, Mehra A, Brass DJ, Labianca G. Network analysis in the social sciences. *Science* 2009;323:892–5.
- [26] Borgatti SP. Identifying sets of key players in a network. *Comput, Math Organ Theory* 2006;12:21–34.
- [27] Onnela J-P, Saramäki J, Hyvönen J, Szabó G, Lazer D, Kaski K, et al. Structure and tie strengths in mobile communication networks. *Proc Natl Acad Sci* 2007;104(18):7332–6.
- [28] Faust K. Comparing social networks: size, density and local structure. *Metodološki zvezki* 2006;3(2):185–216.
- [29] Colizza V, Barrat A, Barthélemy M, Vespignani A. The role of the airline transportation network in the prediction and predictability of global epidemics. *Proc Natl Acad Sci USA* 2006;103(7):2015–20.
- [30] Milo R, Shen-Orr S, Itzkovitz S, Kashtan N, Chklovskii D, Alon U. Network motifs: simple building blocks of complex networks. *Science* 2002;298:824–7.
- [31] Alon U. Biological networks: the tinkerer as an engineer. *Science* 2003;301:1866–7.
- [32] Bollobás B. Random graphs. London: Academic; 1985.
- [33] Cohen R, Erez K, Ben-Avraham D, Havlin S. Breakdown of the internet under intentional attack. *Phys Rev Lett* 2001;86(16):3682.
- [34] Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ. Mitigation of malicious attacks on networks. *Proc Natl Acad Sci* 2011;108(10):3838–41.
- [35] Herrmann HJ, Schneider CM, Moreira AA, Andrade Jr JS, Havlin S. Onion-like network topology enhances robustness against malicious attacks. *J Stat Mech: Theory Exp* 2011;2011(01):P01027.
- [36] Havlin S, Bunde A, Bunde A, Havlin S. Fractals and disordered systems. Springer Berlin; 1991.
- [37] Gao J, Buldyrev SV, Stanley HE, Havlin S. Networks formed from interdependent networks. *Nat Phys* 2012;8(1):40–8.
- [38] Cohen R, Havlin S. Complex networks: structure, robustness and function. Cambridge: Cambridge University Press; 2010.
- [39] Bunde S, Havlin A. Fractals and disordered systems. New York: Springer; 1996.
- [40] Chen Y, Paul G, Havlin S, Liljeros F, Stanley HE. Finding a better immunization strategy. *Phys Rev Lett* 2008;101(5):058701.
- [41] Cohen R, Havlin S, Ben-Avraham D. Efficient immunization strategies for computer networks and populations. *Phys Rev Lett* 2003;91(24):247901.
- [42] Braunstein LA, Buldyrev SV, Cohen R, Havlin S, Stanley HE. Optimal paths in disordered complex networks. *Phys Rev Lett* 2003;91:168701.
- [43] Li D, Fu B, Wang Y, Lu G, Berezin Y, Stanley HE, et al. Percolation transition in dynamical traffic network with evolving critical bottlenecks. *Proc Natl Acad Sci* 2015;112(3):669–72.
- [44] Zimmerman R. Decision-making and the vulnerability of interdependent critical infrastructure. In: Proceedings of the 2004 IEEE International Conference on Systems, Man & Cybernetics 2005;5:4059–63.
- [45] Mendonça D, Wallace WA. Impacts of the 2001 world trade center attack on new york city critical infrastructures. *J Infrastruct Syst* 2006;12(4):260–70.
- [46] Robert B, Morabito L. The operational tools for managing physical interdependencies among critical infrastructures. *Int J Crit Infrastruct* 2008;4(4):353–67.
- [47] Reed DA, Kapur KC, Christie RD. Methodology for assessing the resilience of networked infrastructure. *Syst J*, IEEE 2009;3(2):174–80.
- [48] Mansson D, Thottappillil R, Backstrom M. Methodology for classifying facilities with respect to intentional emi. *IEEE Trans Electromagn Compat* 2009;51(1):46–52.
- [49] Rosato V, Issacharoff L, Tiriticco F, Meloni S, Porcellinis S, Setola R. Modeling interdependent infrastructures using interacting dynamical models. *Int J Crit Infrastruct* 2008;4:63–79.
- [50] D'Agostino G, Scala A. Networks of networks: the last frontier of complexity. Springer; 2014.
- [51] Rinaldi SM, Peerenboom JP, Kelly TK. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Syst, IEEE* 2001;21(6):11–25.
- [52] Gao J, Li D, Havlin S. From a single network to a network of networks. *Nat Sci Rev* 2014;1(3):346–56.
- [53] U.S.-Canada Power System Outage Task Force. Final report on the august 14th 2003 blackout in the united states and canada: causes and recommendations. The Task Force; April 2004. Technical report.
- [54] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature* 2010;464(7291):1025–8.
- [55] Parshani R, Buldyrev SV, Havlin S. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys Rev Lett* 2010;105(4):048701.
- [56] Shao J, Buldyrev SV, Havlin S, Stanley HE. Cascade of failures in coupled network systems with multiple support-dependence relations. *Phys Rev E* 2011;83(3):036116.
- [57] Bashan A, Parshani R, Havlin S. Percolation in networks composed of connectivity and dependency links. *Phys Rev E* 2011;83:051127.
- [58] Zhao J-H, Zhou H-J, Liu Y-Y. Inducing effect on the percolation transition in complex networks. *Nat Commun* 2013;4:2412.
- [59] Leicht EA, D'Souza RM. Percolation on interacting networks. *arXiv:cond-mat/0907089* 2011.
- [60] Parshani R, Rozenblat C, Iettri D, Ducruet C, Havlin S. Inter-similarity between coupled networks. *EPL (Europhys Lett)* 2010;92(6):68002.
- [61] Brummitt CD, DSouza RM, Leicht E. Suppressing cascades of load in interdependent networks. *Proc Natl Acad Sci* 2012;109(12):E680–9.
- [62] Li D, Qin P, Wang H, Liu C, Jiang Y. Epidemics on interconnected lattices. *EPL (Europhys Lett)* 2014;105(6):68004.
- [63] Bashan A, Berezin Y, Buldyrev SV, Havlin S. The extreme vulnerability of interdependent spatially embedded networks. *Nat Phys* 2013;9(10):667–72.
- [64] Berezin Y, Bashan A, Danziger MM, Li D, Havlin S. Localized attacks on spatially embedded networks with dependencies. *Sci Rep* 2015;5(8934).
- [65] Hu Y, Ksherim B, Cohen R, Havlin S. Percolation in interdependent and interconnected networks: abrupt change from second to first order transition. *Phys Rev E* 2011;84:066116.
- [66] Morris RG, Barthélemy M. Transport on coupled spatial networks. *Phys Rev Lett* 2012;109(12):128703.
- [67] Zhang P, Cheng B, Zhao Z, Li D, Lu G, Wang Y, et al. The robustness of interdependent transportation networks under targeted attack. *EPL (Europhys Lett)* 2013;103(6):68005.
- [68] Gomez S, Diaz-Guilera A, Gomez-Gardeñes JG-G, Perez-Vicente CJ, Moreno Y, Arenas A. Diffusion dynamics on multiplex networks. *Phys Rev Lett* 2013;110(2):028701.



- [69] Nagler J, Levina A, Timme M. Impact of single links in competitive percolation. *Nat Phys* 2011;7(3):265–70.
- [70] Aguirre J, Papo D, Buldú JM. Successful strategies for competing networks. *Nat Phys* 2013;9(4):230–4.
- [71] Kivela M, Arenas A, Barthelemy M, Gleeson JP, Moreno Y, Porter MA. Multilayer networks. *arXiv preprint arXiv:13097233* 2013.
- [72] Radicchi F, Arenas A. Abrupt transition in the structural formation of interconnected networks. *Nat Phys* 2013;9(11):717–20.
- [73] Baxter G, Dorogovtsev S, Goltsev A, Mendes J. Avalanche collapse of interdependent networks. *Phys Rev Lett* 2012;109(24):248701.
- [74] Dong G, Gao J, Du R, Tian L, Stanley HE, Havlin S. Robustness of network of networks under targeted attack. *Phys Rev E* 2013;87(5):052804.
- [75] Pocock MJ, Evans DM, Memmott J. The robustness and restoration of a network of ecological networks. *Science* 2012;335(6071):973–7.
- [76] Newman ME, Strogatz SH, Watts DJ. Random graphs with arbitrary degree distributions and their applications. *Phys Rev E* 2001;64(2):026118.
- [77] Shao J, Buldyrev SV, Braunstein LA, Havlin S, Stanley HE. Structure of shells in complex networks. *Phys Rev E* 2009;80(3):036105.
- [78] Gao J, Buldyrev SV, Havlin S, Stanley HE. Robustness of a network of networks. *Phys Rev Lett* 2011;107(19):195701.
- [79] Gao J, Buldyrev SV, Havlin S, Stanley HE. Robustness of a network formed by  $n$  interdependent networks with a one-to-one correspondence of dependent nodes. *Phys Rev E* 2012;85(6):066134.
- [80] Son S-W, Bizhani G, Christensen C, Grassberger P, Paczuski M. Percolation theory on interdependent networks based on epidemic spreading. *EPL (Europhys Lett)* 2012;97(1):16006.
- [81] Gao J, Buldyrev SV, Stanley HE, Xu X, Havlin S. Percolation of a general network of networks. *Phys Rev E* 2013;88(6):062816.
- [82] Huang X, Gao J, Buldyrev SV, Havlin S, Stanley HE. Robustness of interdependent networks under targeted attack. *Phys Rev E* 2011;83(6):065101.
- [83] Dong G, Gao J, Tian L, Du R, He Y. Percolation of partially interdependent networks under targeted attack. *Phys Rev E* 2012;85(1):016112.
- [84] Huang X, Vodenska I, Havlin S, Stanley HE. Cascading failures in bipartite graphs: model for systemic risk propagation. *Sci Rep* 2013;3.
- [85] Radicchi F. Percolation in real interdependent networks. *Nat Phys* 2015;11:597–602.
- [86] Reis SD, Hu Y, Babino A, Andrade Jr JS, Canals S, Sigman M, et al. Avoiding catastrophic failure in correlated networks of networks. *Nat Phys* 2014;10:762–7.
- [87] Hu Y, Havlin S, Makse HA. Conditions for viral influence spreading through multiplex correlated social networks. *Phys Rev X* 2014;4(2):021031.
- [88] Buldyrev SV, Shere NW, Cwlich GA. Interdependent networks with identical degrees of mutually dependent nodes. *Phys Rev E* 2011;83(1):016112.
- [89] Cellai D, López E, Zhou J, Gleeson JP, Bianconi G. Percolation in multiplex networks with overlap. *Phys Rev E* 2013;88(5):052811.
- [90] Hu Y, Zhou D, Zhang R, Han Z, Rozenblat C, Havlin S. Percolation of interdependent networks with intersimilarity. *Phys Rev E* 2013;88(5):052805.
- [91] Liu Y-Y, Slotine J-J, Barabási A-L. Controllability of complex networks. *Nature* May 2011;473:167–73.
- [92] Gao J, Liu Y-Y, D'Souza RM, Barabási A-L. Target control of complex networks. *Nat Commun* 2014;5.
- [93] Jia T, Liu Y-Y, Csóka E, Pósfai M, Slotine J-J, Barabási A-L. Emergence of bimodality in controlling complex networks. *Nat Commun* 2013;4.
- [94] Jia T, Barabási A-L. Control capacity and a random sampling method in exploring controllability of complex networks. *Sci Rep* 2013;3.
- [95] Jia T, Pósfai M. Connecting core percolation and controllability of complex networks. *Sci Rep* 2014;4.
- [96] Cowan NJ, Chastain EJ, Vilhena DA, Freudenberg JS, Bergstrom CT. Nodal dynamics, not degree distributions, determine the structural controllability of complex networks. *PLoS One* 2012;7(6):e38398.
- [97] Yan G, Ren J, Lai Y-C, Li C-H, Li B. Controlling complex networks: how much energy is needed? *Phys Rev Lett* 2012;108(21):218703.
- [98] Nepusz T, Vicsek T. Controlling edge dynamics in complex networks. *Nat Phys* 2012;8(7):568–73.
- [99] Nicosia V, Criado R, Romance M, Russo G, Latora V. Controlling centrality in complex networks. *Sci Rep* 2012;2.
- [100] Liu X, Pan L. Detection of driver metabolites in the human liver metabolic network using structural controllability analysis. *BMC Syst Biol* 2014;8(1):51.
- [101] Liu X, Pan L. Identifying driver nodes in the human signaling network using structural controllability analysis. *Comput Biol Bioinf, IEEE/ACM Trans* 2015;12(2):467–72.
- [102] Wang W-X, Ni X, Lai Y-C, Grebogi C. Optimizing controllability of complex networks by minimum structural perturbations. *Phys Rev E* 2012;85(2):026115.
- [103] Yan G, Tsekenis G, Barzel B, Slotine J-J, Liu Y-Y, Barabási A-L. Spectrum of controlling and observing complex networks. *arXiv preprint arXiv:150301160* 2015.
- [104] Pósfai M, Hövel P. Structural controllability of temporal networks. *N J Phys* 2014;16(12):123055.
- [105] Cohen R, Erez K, Ben-Avraham D, Havlin S. Breakdown of the internet under intentional attack. *Phys Rev Lett* 2001;86:3682–5.
- [106] Gallos LK, Cohen R, Argyrakis P, Bunde A, Havlin S. Stability and topology of scale-free networks under attack and defense strategies. *Phys Rev Lett* 2005;94(18):188701.
- [107] Kenett DY, Gao J, Huang X, Shao S, Vodenska I, Buldyrev SV, et al. Network of interdependent networks: overview of theory and applications. *Proceedings of the Networks of Networks: The Last Frontier of Complexity*. Springer; 2014. p. 3–36.
- [108] Furfine CH. Interbank exposures: quantifying the risk of contagion. *J Money, Credit Banking* 2003;111–28.
- [109] Upper C, Worms A. Estimating bilateral exposures in the german interbank market: is there a danger of contagion? *Eur Econ Rev* 2004;48(4):827–49.
- [110] Nier E, Yang J, Yorulmazer T, Alentorn A. Network models and financial stability. *J Econ Dyn Control* 2007;31(6):2033–60.
- [111] Cifuentes R, Ferrucci G, Shin HS. Liquidity risk and contagion. *J Eur Econ Assoc* 2005;3:556.
- [112] Dosenbach NU, Fair DA, Miezin FM, Cohen AL, Wenger KK, Dosenbach RA, et al. Distinct brain networks for adaptive and stable task control in humans. *Proc Natl Acad Sci* 2007;104(26):11073–8.
- [113] Barabási A-L. The network takeover. *Nat Phys* 2011;8:14–16.
- [114] Strogatz SH. Exploring complex networks. *Nature* March 2001;410:268–76.
- [115] Albert R, Barabási A-L. Statistical mechanics of complex networks. *Rev Mod Phys* Jan 2002;74(1):47–97.
- [116] Pan Y, Li X. Structural controllability and controlling centrality of temporal networks. *PLoS One* 2014;e94998(4).
- [117] Nie S, Wang X, Wang B. Effect of degree correlation on exact controllability of multiplex networks. *Phys A: Stat Mech Appl* 2015;436:98–102.
- [118] Yuan Z, Zhao C, Wang W-X, Di Z, Lai Y-C. Exact controllability of multiplex networks. *N J Phys* 2014;16(10):103036.
- [119] Zhang Y, Garas A, Schweitzer F. The value of peripheral nodes in controlling multilayer networks. *arXiv preprint arXiv:150602963* 2015.
- [120] Wang L, Chen G, Wang XF, Tang WK. Controllability of networked mimo systems. *arXiv preprint arXiv:150501255* 2015.
- [121] Kalman RE. Mathematical description of linear dynamical systems. *J Soc Ind Appl Math, Ser A: Control* 1963;1(2):152–92.
- [122] Slotine J-J E, Li W, et al. *Applied nonlinear control*, volume 199. NJ: Prentice-hall Englewood Cliffs; 1991.
- [123] Lin CT. Structural controllability. *IEEE Trans Autom Control*, 1974;19(3):201–8.
- [124] Lohmiller W, Slotine J-J E. On contraction analysis for non-linear systems. *Automatica* 1998;34(6):683–96.
- [125] Hopcroft JE, Karp RM. An  $n^{5/2}$  algorithm for maximum matchings in bipartite graphs. *SIAM J Comput* 1973;2(4):225–31.
- [126] Liu Y-Y, Slotine J-J, Barabási A-L. Control centrality and hierarchical structure in complex networks. *PLoS One* 2012;e44459(9).
- [127] Jiang Z-Q, Xie W-J, Li M-X, Podobnik B, Zhou W-X, Stanley HE. Calling patterns in human communication dynamics. *Proc Natl Acad Sci* 2013;110(5):1600–5.
- [128] Barigozzi M, Fagiolo G, Garlaschelli D. Multinetwork of international trade: A commodity-specific analysis. *Phys Rev E* 2010;81(4):046104.
- [129] Barabási A-L. The origin of bursts and heavy tails in human dynamics. *Nature* 2005;435(7039):207–11.
- [130] Malmgren RD, Stouffer DB, Motter AE, Amaral LA. A poissonian explanation for heavy tails in e-mail communication. *Proc Natl Acad Sci* 2008;105(47):18153–8.
- [131] Zhou D, Bashan A, Cohen R, Berezin Y, Shnerb N, Havlin S. Simultaneous first- and second-order percolation transitions in interdependent networks. *Phys Rev E* 2014;90(1):012803.