

Chapter 2

Optimizing Network Topology for Cascade Resilience

Alexander Gutfraind

Abstract Complex networks need resilience to cascades – to prevent the failure of a single node from causing a far-reaching domino effect. Such resilience can be achieved actively or topologically. In active resilience schemes, sensors detect the cascade and trigger responses that protect the network against further damage. In topological resilience schemes, the network’s connectivity alone provides resilience by dissipating nascent cascades. Designing topologically resilient networks is a multi-objective discrete optimization problem, where the objectives include resisting cascades and efficiently performing a mission. Remarkably, terrorist networks and other “dark networks” have already discovered how to design such networks. While topological resilience is more robust than active resilience, it should not always be pursued because in some situations it requires excessive loss of network efficiency.

2.1 Introduction

Cascades are ubiquitous in complex networks and they have inspired much research in modeling, prediction and mitigation [11, 14, 20, 35, 53, 54, 57, 60, 62, 72]. For example, since many infectious diseases spread over contact networks a single carrier might infect other individuals with whom she interacts. The infection might then propagate widely through the network, leading to an epidemic. Even if no lives are lost, recovery may require both prolonged hospitalizations and expensive treatments. Similar cascade phenomena are found in other domains such as power distribution systems [22, 38, 43], computer networks such as ad-hoc

A. Gutfraind

Center for Nonlinear Studies and T-5/D-6, Los Alamos National Laboratory,
Los Alamos, NM 87545, USA

e-mail: mailto:agutfraind.research@gmail.com

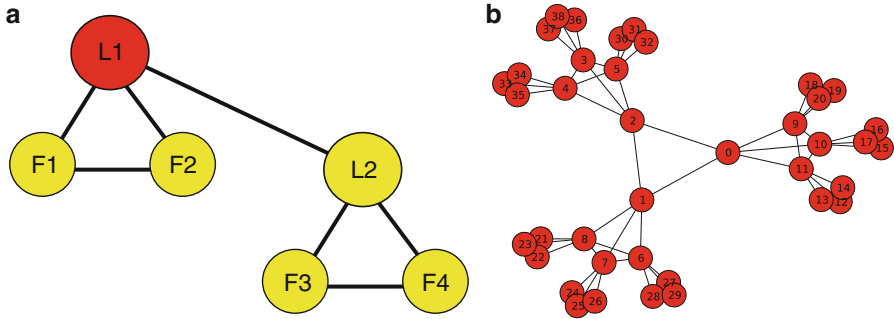


Fig. 2.1 The French World-War II underground network *Franco-tireurs et Partisans* (FTP) reconstructed by the author based on the account in [51]. Its organizational unit was the combat group (a). In an idealized case, not always followed, this was divided into two “teams” of three fighters, where leader L1 was in overall command and in command of team 1. His lieutenant, L2, led team 2 and assumed overall command if L1 was captured. The small degree of the nodes ensured that the capture of any one node did not risk the exposure of a significant fraction of the organization. Each “group” is in a command hierarchy (b) where three groups (bottom-level nodes) made a “section,” three sections made a “company,” and finally three companies made a “battalion”

wireless networks [60], financial markets [8, 36], and socio-economic systems [40]. A particularly interesting class are “dark” or clandestine social networks, such as terrorist networks, guerrilla groups [65], espionage, and crime rings [5, 52]. In such networks, if one of the nodes (i.e. individuals) is captured by law enforcement agencies, he may betray all the nodes connected to him leading to their likely capture.

Dark networks are therefore designed to operate in conditions of intense cascade pressure. As such they can serve as useful prototypes of networks that are cascade-resilient because of their connectivity structure (topology) alone. Their nodes are often placed in well-defined cells – closely-connected subnetworks with only sparse connections to the outside (for an example from World War II see Fig. 2.1) [51]. The advantages of cells are thought to be that the risk from the capture of any person is mostly limited to his or her cell mates, thereby protecting the rest of the network [29, 48]. Modern terrorist groups retain this cellular structure, but increasingly use networks made of components with no connections between them, thus caging cascades within each component [67, 69, 73].

2.1.1 Active vs. Topological Cascade Resilience

Networks could be endowed with cascade resilience using two complementary approaches: “active” and “topological.” In active resilience, the network is monitored for cascades, and if a cascade is detected, attempts are made to stop it *while it progresses*. For example, in case of human pathogens, health authorities may continuously monitor hospital records for contagious diseases. If the records begin

to show anomalous increases, various responses are initiated, including distribution of medicines and alerts to the public. Similarly, in power distribution systems, special devices monitor the network for signs of cascades, such as high currents or phase changes. Those may indicate failures in lines, short circuits and other phenomena that threaten to disrupt the system or damage its components. The power system includes a variety of automated controls tasked with stopping the nascent cascade [53], such as “relays.” Those relays can automatically shut down faulty lines or nodes of the network so as to isolate them from the rest of the network [63, 75].

Those two examples of active cascade resilience must be contrasted with “topological” approach to resilience where only the topology (i.e. the pattern of connections) is used to increase cascade resilience. For example, the network could be structured into modules, where any two modules are connected to each other through long paths. As a result, in certain types of cascades, a failure in one module might dissipate before it reaches any other module. When topological cascade resilience is possible, it offers two advantages over active resilience: simplicity and robustness. In topological resilience, the network protects itself, requiring no real-time automated decisions or difficult-to-achieve rapid response during the cascade.

2.2 What is a Cascade-Resilient Network?

The words Network, Cascade, and Resilience have many domains of application, so much so that no universal definition of these terms exists. Therefore, this section briefly surveys some of the recurrent applications and meanings of those terms. It also introduces specific definitions that are appropriate for some applications. Later in the paper these definitions serve as an example of optimizing networks for cascade resilience.

2.2.1 *Network as an Unweighted Graph*

Complex Networks is the study of real world systems using ideas of graph theory. Specifically, here and in most other studies the network is represented using simple unweighted graph G : a tuple (V, E) where V is a set called “nodes” or “vertices” and E are unordered two-element subsets of V termed “edges.” Such an approach offers simplicity and can employ the well-developed tools of graph theory. Ultimately, though, models of networks must consider their evolving nature, fuzzy boundaries, and multiplicities of node classes and diverse relationships.

The simplification is often unavoidable given the lack of data on networks. For example, in dark social networks only the connectivity is known, if that. Fortunately, the loss of information involved in representing networks as simple rather than say, as weighted graphs, could be evaluated. It is shown in Sect. 2.3.1 that at least in two examples where the weights are known, the error in key metrics when using simple graphs has no systematic bias and is usually small.

2.2.2 *Cascades*

There is a very extensive literature on both cascades and resilience. The classic literature on cascades includes two basic models: percolation cascades and capacity cascades. The former originate in Physics but are often applied to Epidemiology, where they are termed “contagions” or “epidemics” (see e.g. [58]). In percolation phenomena, nodes are assigned states which change because of the influence of their neighbors. For example, an infected node can pass the infection to its contacts in the network, and the infection could then be passed to more and more nodes. Another variant of such percolations are the case where nodes change their state only when a certain fraction of their neighbors exert influence (see e.g. [14, 72]). Percolation phenomena are exceptionally well-studied, and in many variants analytic expressions exist for the final extent of the cascade as a function of the network topology (see e.g. [26, 57]). The capacity cascades are characteristic of capacitated networks, such as power transmission systems and supply chains. Classically, in those systems the edges are assigned capacities and thus carry flows from supply nodes to demand nodes. Cascades occur when due to failures the flow can no longer be carried by the edges within their capacities or when some of the supply nodes fail [3, 21, 43, 53]. In capacity cascades the failure can jump to nodes that are many hops away from the initial failures possibly skipping the neighbors.

2.2.3 *Resilience*

A vast number of studies attempted to define resilience, often in very different ways. Perhaps the most common meaning refers to the connectivity of the network under disruption or failures in its components. Such definitions are motivated by applications in telecommunications where it is desired that nodes are able to find a path to each other even if some of the components in the networks are damaged or destroyed [1, 6, 7, 12, 15, 16, 23, 33, 34, 41].

The idea of damaging networks has attracted a lot of research in the area of Sociology of secret societies such as terrorist networks [4, 25, 29, 32, 48, 49, 52, 74]. In fact, many secret societies are benign, including non-governmental organizations and dissident movements operating in hostile political environments. In those networks, if the network is penetrated by its enemy, it must be able to minimize the damage. Economists too have recently analyzed the problem of organizational design when the organization is being attacked [27]. Related problems have also been studied by epidemiologists, where the question focused on immunization strategies (e.g. [64]) but apparently not as a question of optimal network design.

Recently, resilience has become associated with the ability to quickly recover from damage rather than to absorb it [10]. Indeed, in many applications disruptions and failures are not rare singular events, but rather occur regularly and even

continuously. For example, there are continuous demand spikes in communication networks [19] and voltage fluctuations in power systems.

It is to be expected that no notion of resilience would be useful universally across different applications. Similarly, many networks experience cascades, but the details vary. This paper will investigate cascade resilience under a particularly important and well-characterized class of cascades known as “susceptible-infected-recovered” (SIR). SIR are a type of cascades where any failed node leads to the failure of each neighboring node independently with probability τ [58]. This τ represents the network’s propensity to experience cascades, expressing both the susceptibility of components and the environment in which the network operates. Using the SIR model, resilience $R(G)$ could be defined as the average fraction of the network that does not fail in the cascade:

$$R(G) = 1 - \frac{1}{n-1} \mathbb{E}[\text{extent of a cascade}], \quad (2.1)$$

where “extent of a cascade” refers to the ultimate number of new cases created by a single failed node (the initial node does not count) and where $n = |V|$ is the number of nodes. For simplicity, cascades are assumed to start at all nodes with uniform probability.

Observe that under this definition the most cascade-resilient network ($R(G) = 1$) is the network with no edges. But such a network cannot carry any information from node to node! It is not surprising that the objective of designing cascade resilience conflicts with other features of the network. In other cascade types, such as cascades on capacitated networks, the most cascade-resilient network might be the network with infinite capacities, which obviously would conflict with the objective of minimizing cost. It follows then that optimization of networks requires specifying a notion of value or efficiency.

2.2.4 Measuring Efficiency

Notions of network efficiency attempt to quantify the value of a network, and this problem has a long history. For example, an influential early work on communication networks suggested that a network’s value increases as $O\left(\frac{n(n-1)}{2}\right)$, because each node can connect to $n-1$ other nodes [9]. However, this measure ignores the difficulty of connecting to other nodes (as well as, e.g. cost). Indeed, it is often desired that the distances between the nodes are short: when nodes are separated by short distances they can, e.g., more easily communicate and distribute resources to each other. Therefore, many authors invoke measures based on the distances between pairs of nodes in the network (see e.g. [44, 49, 55]).

In the following we will consider a version of distance-based efficiency, termed “distance-attenuated reach” metric [44]. For all pairs of nodes $u, v \in V$, weigh each

pair by the inverse of its internal distance (the number of edges in the shortest path from u to v) taken to power g :

$$W(G) = \frac{1}{n(n-1)} \sum_{u \in V} \sum_{v \in V \setminus \{u\}} \frac{1}{d(u,v)^g}, \quad (2.2)$$

Normalization by $n(n-1)$ ensures that $0 \leq W(G) \leq 1$, and only the complete graph achieves 1. As usual, for any node v with no path to u , set $\frac{1}{d(u,v)^g} = 0$. The parameter g , “connectivity attenuation” represents the rate at which distance decreases the connectivity between nodes. Unless stated otherwise $g = 1$. A valuable property of $W(G)$ is that it is well-defined and non-singular even on networks that have multiple components with no connections to each other. As will be shown, such a separation into components provides a very powerful mechanism for cascade resilience.

2.3 Evaluating Real Networks

Significant insight into cascade resilience can be derived from comparing the cascade resilience of networks from different domains. We will see that dark networks like terrorist networks are more successful in the presence of certain cascades than other complex networks. Their success stems not from cascade resilience alone but from balancing resilience with efficiency.

To make those comparisons, define the overall “fitness,” $F(G)$, of a network by aggregating resilience and efficiency through a weight parameter r :

$$F(G) = rR(G) + (1-r)W(G).$$

The parameter r depends on the application and represents the damage from a cascade – from light ($r \rightarrow 0$) to catastrophic ($r \rightarrow 1$). Note that it is possible to include in fitness other metrics such as construction cost.

We will compare the fitnesses of several complex networks, including communication, infrastructure and scientific networks to the fitnesses of dark networks. The class of dark networks will be represented by three networks: the 9/11, 11M and FTP networks. The 9/11 network links the group of individuals who were directly involved in the September 11, 2001 attacks on New York and Washington, DC [49]. Similarly the 11M network links those responsible for the March 11, 2004 train attacks in Madrid [67]. Both 9/11 and 11M were constructed from press reports of the attacks. Edges in those networks connect two individuals who worked with each other in the plots [49, 67]. The FTP network is an underground group from World War II (Fig. 2.1), whose network was constructed by the author from a historical account [51].

Figure 2.2 shows that the dark networks attain the highest fitness values of all networks, except for extreme levels of cascade risk ($\tau > 0.6$) This is to be expected:

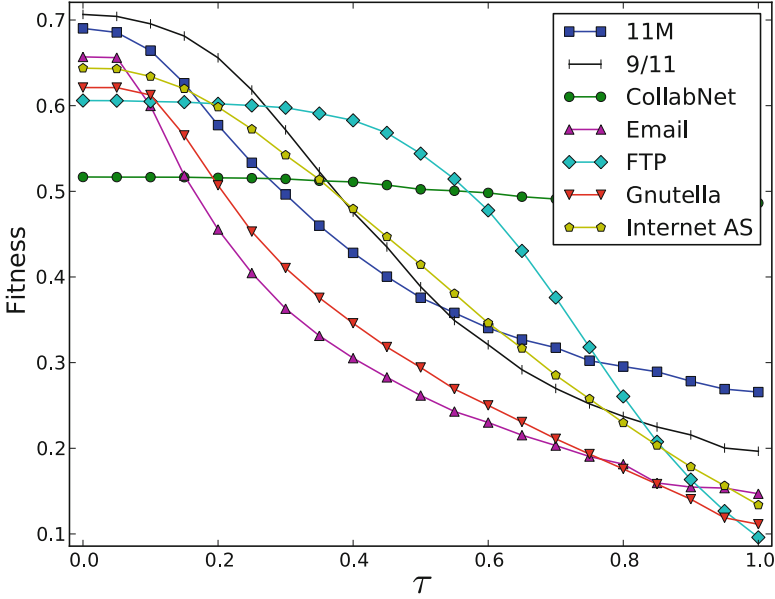


Fig. 2.2 Fitnesses of various networks at $r = 0.51$ and various values of τ . 11M is the network responsible for the March 11, 2004 attacks in Madrid (70 nodes, 240 edges). 9/11 [49] is the network responsible for the 9/11 attacks (62 nodes, 152 edges). CollabNet [59] is a scientific co-authorship network in the area of network science (1,589 nodes, 2,742 edges). E-Mail [28] is a university's e-mail contact network, showing its organizational structure (1,133 nodes, 5,452 edges). FTP is the network in Fig. 2.1 (174 nodes, 300 edges). Gnutella [37,66] is a snapshot of the peer-to-peer network (6,301 nodes, 20,777 edges). Internet AS [47] is a snapshot of the Internet at the autonomous system level (26,475 nodes, 53,381 edges). Except for $\tau > 0.6$ dark networks (11M, 9/11 and FTP) attain the highest fitness

only 11M, 9/11, and the FTP networks have been designed with cascade resilience as a significant criterion – a property that makes them useful case studies. For high cascade risks ($\tau > 0.6$) the CollabNet network exceeds the fitnesses of the dark networks. CollabNet was drawn by linking scientists who co-authored a paper in the area of network science [59]. It achieved high fitness because it is partitioned into research groups that have no publications with outside scientists. Like some terrorist networks, it is separated into entirely disconnected cells.

It is interesting to compare the empirical networks to each other in their efficiency and resilience (Fig. 2.3). Note that FTP and 9/11 networks are not the most resilient, but they strike a good balance between resilience and efficiency. The advantages of the two networks over other networks are not marginal, implying that their advantages in fitness are not sensitive to the choice of r . Of course, they are optimized for particular combinations of r and τ , and will no longer be very successful outside that range. For instance, in the range of high r and high τ networks with multiple connected components would have higher fitness because they are able to isolate cascades in one component.

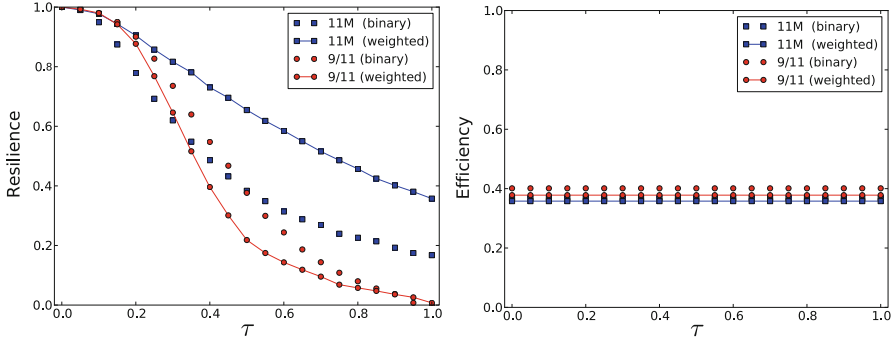


Fig. 2.3 Resilience and efficiency of the real networks. The fittest networks are not always the most resilient

The 9/11 and the 11M networks are very successful for low values of τ (< 0.2), but then rapidly deteriorate because of a jump in the extent of cascades – the so-called percolation transition [24]. Past this threshold, cascades start affecting a large fraction of the network, resilience collapses and the fitness declines rapidly. The pattern of onset of failure can be clearly seen in most of the networks. For violent secret societies this transition means that the network might be initially hard to defeat, but there is a point after which efforts against it start to pay off. Because τ is representative of the security environment, the 9/11 network is found to be relatively ill-adapted to the more stringent security regime implemented after the attacks. Indeed, it is likely that the 9/11 attacks would have been thwarted under the current security regime since some of the nodes were captured before the attacks, but not interrogated in time to discover and apprehend the rest of the network [71]. In contrast, the cellular tree hierarchy of the FTP network is more suitable for an intermediate range of cascade risks. However, the pair-wise distances in it are too long to provide high efficiency. Therefore, its fitness is comparatively poor under very low and very high values of τ .

2.3.1 Resilience and Efficiency of Weighted Networks

In some networks, each edge (u, v) carries a distance weight $D_{uv} > 0$. The smaller the distance, the closer the connection between u and v . We now explain in some detail how to compute the fitness of those networks. We will introduce generalizations of resilience and efficiency, that reduce to the original definitions for unweighted networks when $D_{uv} = 1$, while capturing the effects of weights in the weighted networks.

The original definition of resilience was built on a percolation model where the failure of any node leads to the failure of its neighbor with probability τ . In the

weighted network, more distant nodes should be less likely to spread the cascade. Thus, we make the probability of cascade through (u, v) to be $\min(\tau/D_{uv}, 1)$.

The efficiency was originally defined as the sum of all-pairs inverse geodesic distances, normalized by the efficiency of the complete graph. In the weighted network, both the distance and the normalization must be generalized. To compute the distance $d(u, v)$ we consider the weights on the edges D and apply Dijkstra's algorithm to find the shortest path. Normalization too must consider D because a weighted graph with sufficiently small distances could outperform the complete graph (if all the edges of the latter have $D_{ij} = 1$). Therefore, we weigh the efficiency by the harmonic mean H of the edges (E) of the graph:

$$W(G) = \frac{H(G)}{n(n-1)} \sum_{u \in V} \sum_{v \in V \setminus \{u\}} \frac{1}{d(u, v)^g}, \quad (2.3)$$

where

$$H(G) = \frac{|E|}{\sum_{(u,v) \in E} \left(\frac{1}{D_{uv}}\right)^g}.$$

The harmonic mean ensures that for any D , the complete graph has $W(G) = 1$.

Having defined generalized resilience and efficiency we can evaluate the standard approach to dark networks, which represents them as binary graphs $D_{uv} \in \{0, 1\}$, rather than as weighted graphs. The former approach is often taken because the information about dark networks is limited and insufficient to estimate edge weights.

Fortunately, in two cases, the 9/11 network and the 11M network [49, 67] the weights could be estimated. The 9/11 data labels nodes as either facilitators or hijackers. Hijackers must train together and thus should tend to have a closer relationship. Thus set $D_{uv} = 2, 1, 0.5$ if the pair u, v includes zero, one or two hijackers, respectively. The 11M network is already weighted ($Z_{uv} = 1, 2, 3, \dots$) based on the number of functions each contact (u, v) serves (friendship, kin, joint training etc.). We mapped those weights to D by $D_{uv} = 2/Z_{uv}$. In both networks, the transformation was so that the weakest ties have weight 2, giving them greater distance than in the binary network, while the strongest ties are shorter than in the binary network.

Figure 2.4 compares the fitnesses, resiliences and efficiencies of the weighted and binary representations. It shows that for both networks, the fitnesses of the binary representation lies within 0.15 of the fitness of the weighted representation and for some τ much closer. The efficiency measures are even more close (within 0.05). The behavior of resilience is intriguing: for the 9/11 network the weighted representation shows more gradual decline as a function of cascade risk when compared to the binary representation. For the 11M network, the decline is actually slightly more sharp in the weighted representation. Structurally, the 11M network has a center (measured by betweenness centrality) of tightly knit-nodes (very short distances), while the 9/11 network is more sparse at its center, increasing its cascade resilience. This effect explains the direction of the error in the binary representation. Based on those two examples, it appears that the binary representation does not have a systematic bias, and may even underestimate the fitness of dark networks.

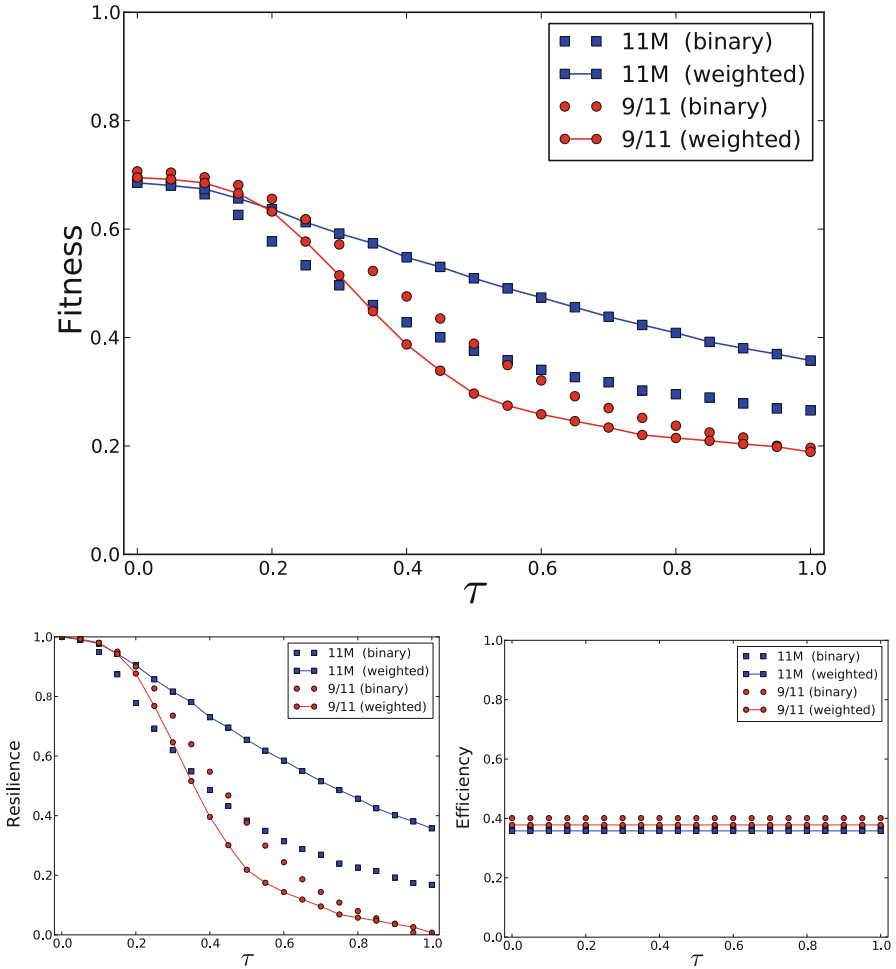


Fig. 2.4 Fitness, resilience, and efficiency of two dark networks ($r = 0.51$), comparing binary and weighted representations. The binary representation matches the weighted representation within 0.15, and typically closer

2.4 Designing Networks

The success of dark networks must be due to structural elements of those networks, such as cells. If identified, those elements could be used to design more resilient networks and to upgrade existing ones. Thus, by learning how dark networks organize, it will be possible to make networks such as communication systems, financial networks, and others more resilient and efficient.

Those identification and design problems are our next task: both will be solved using an approach based on discrete optimization. Let a set of graphs \mathbb{G} be called a

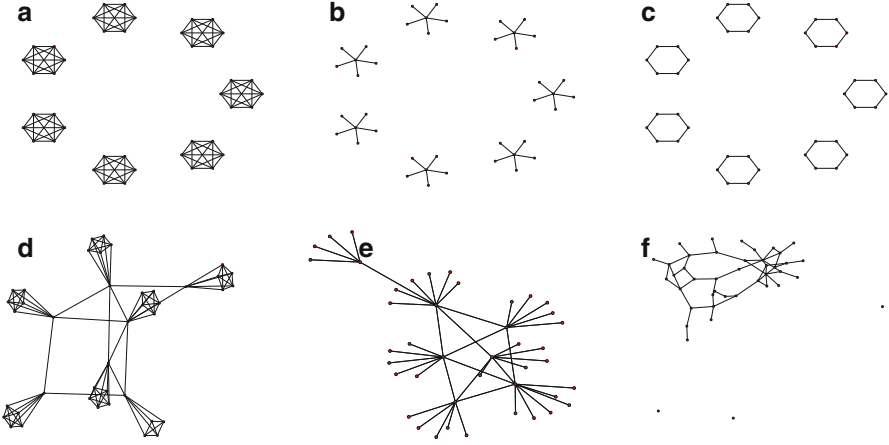


Fig. 2.5 Graphs illustrating the 6 network designs. *Cliques* (a), *Stars* (b), *Cycles* (c), *Connected Cliques* (d), *Connected Stars* (e), and *Erdos-Renyi “ER”* (f). Each design is configured by just one or two parameters (the number of individuals per cell and/or the random connectivity). This enables rapid solution of the optimization problem. In computations the networks were larger ($n = 180$ nodes)

“network design” if all the networks in it share a structural element. Since dark networks are often based on dense cliques, we consider a design where all the networks consist of one or multiple cliques. We consider also designs based on star-like cells, cycle-based cells and more complex patterns (see Fig. 2.5).

In the first step, we will find the most successful network within each design. Namely, consider an optimization problem where the decision variable is the topology G of a simple graph taken from a design \mathbb{G} . The objective is the fitness $F(G)$:

$$\max_{G \in \mathbb{G}} F(G). \quad (2.4)$$

In the second step, we will compare the fitnesses across designs, thus identifying the topological feature with the highest fitness (e.g. star vs. clique).

This optimization problem introduces a method for designing cascade-resilient networks for applications such as vital infrastructure networks. To apply this to a given application, one must make the design \mathbb{G} the set of all feasible networks in that domain, to the extent possible by computational constraints. For a related approach using game-theoretic ideas see Lindelauf et al. [48, 49].

A complementary approach is to consider the multi-objective optimization problem in which $R(G)$ and $W(G)$ are maximized simultaneously:

$$\max_{G \in \mathbb{G}} \{R(G), W(G)\}. \quad (2.5)$$

The multi-objective approach cannot find the optimal network but instead produces the Pareto frontier of each design – the set of network configurations that cannot be

improved without sacrificing either efficiency or resilience. The decision maker can use the frontier to make the optimal trade-off between resilience and efficiency.

The fitness and the multi-objective optimization approaches could be easily generalized to consider additional design objectives and constraints. For example, research on social networks indicates that resilience and efficiency might be just two of several design criteria that also include, e.g. “information-processing requirements,” that impose additional constraints on network designs [5]. In the original context, “information-processing” refers to the need to have ties between individuals involved in a particular task, when the task has high complexity. Each individual might have a unique set of expertise into which all the other agents must tap directly. Generalizing from sociology, such “functional constraints” might considerably limit the flexibility in constructing resilient and efficient networks. For example, in the context of terrorism, this constraint significantly decreased the quality of attacks that could be successfully carried out in the post 9/11 security environment [73]. Such functional constraints could be addressed by looking at a palette of network designs which already incorporate such constraints. In engineering applications, such as infrastructure or communication networks, the financial cost of building the network is another key objective.

2.4.1 Properties of the Solution

The solution to the scalarized objective problem, (2.4) has a number of useful properties: Its fitness is continuous in the parameter r and changes predictably with other parameters: Notice that the claim is not about the continuity of fitness of a single configuration as a function of r but rather about the set of optimal solutions.

Proposition 2.1. $f(r) = \max_{G \in \mathbb{G}} F(G, r)$ is Lipschitz-continuous for $r \in [0, 1]$.

Proof. The argument constructs a bound on the change in f in terms of the change in r . Consider an optimal configuration C_1 of a design for $r = r_1$ and let its fitness be $f_1 = F(C_1, r_1)$ (there is slight abuse of notation since C is a configuration, whose fitness is the average fitness of an ensemble of graphs).

Observation 1: Consider the fitness of C_1 at $r = r_2$. Because C_1 is fixed and the metrics are bounded ($0 \leq R \leq 1$ and $0 \leq W \leq 1$), the fitness change is bounded by the change in r :

$$\begin{aligned} |f_1 - F(C_1, r_2)| &= |r_1 R(C_1) + (1 - r_1) W(C_1) \\ &\quad - r_2 R(C_1) - (1 - r_2) W(C_1)| \\ &= |(r_1 - r_2) R(C_1) - (r_1 - r_2) W(C_1)| \\ &\leq |r_1 - r_2|. \end{aligned}$$

Observation 2: Let C_2 be the optimal configuration for $r = r_2$ and let $f_2 = F(C_2, r_2)$. Since C_2 is optimal for $r = r_2$ it satisfies: $f_2 \geq f(C_1, r_2)$, and so $-f_2 \leq -F(C_1, r_2)$. It follows that $f_1 - f_2 \leq f_1 - F(C_1, r_2)$. Take the absolute value of the right hand side and apply Observation 1 to get the bound: $f_1 - f_2 \leq |r_1 - r_2|$.

Observation 3: Applying the argument of Observations 1&2 but reversing the roles of C_1 and C_2 implies that $f_2 - f_1 \leq |r_1 - r_2|$.

Observations 2 and 3 give $|f_1 - f_2| \leq |r_1 - r_2|$, proving the result.

Proposition 2.2. *Let $f(\tau)$ be the highest attainable fitness within a fixed network design \mathbb{G} , for cascade probability τ :*

$$f(\tau) = \max_{G \in \mathbb{G}} \left[\underbrace{rR(G, \tau) + (1-r)W(G)}_{F(G, \tau)} \right]$$

Then $f(\tau)$ is a non-increasing function of τ .

Proof. The proof relies on the simple claim that resilience of networks does not increase when τ increases [31]. The claim is equivalent to the result that for a given graph G increasing τ does not decrease the expected extent of cascades. The remainder is almost trivial: it is the claim that when the fitness of all the points on the space (all graphs) has been made smaller or kept the same (by increasing τ), the new maximum value would not be greater than in the old space.

The argument is easy to generalize. One could apply this method to the parameter g of attenuation, showing that fitness is non-increasing when attenuation is increased.

2.4.2 General Approaches to Large-Scale Networks

Our study did not involve solving the general optimization problem of finding the optimal network on n nodes in (2.4), but in some cases solving the general problem would be required. Clearly, the multi-objective problem and the scalarized model are hard: both are discrete optimization problems with non-linear objective functions. In general, solutions could be obtained using derivative-free optimization methods [18] and approximations such as [38, 68]. Promising approaches also exist for finding the Pareto front [45, 50, 56]. Whether those methods are fast and accurate enough would depend on the definitions of $R(G)$, $W(G)$ and the set \mathbb{G} .

In small instances, it might also be possible to use the following approach based on bilevel stochastic integer programming. Given a specified network size (e.g. 180 nodes), one has integer decision variables $E_{ij} \in \{0, 1\}$ for all $i \neq j$ where $i, j \in V$. The objective contains a stochastic term, $R(G)$ and a deterministic term, $W(G)$. The former is a linear function of the expected extent of percolation cascades. The cascade extents could be computed by generating stochastic starting points

$s \sim \text{Uniform}[V]$ and stochastic edge connectivity values $B_{ij} \sim \text{Bin}(\tau)$ for all i, j with $E_{ij} = 1$. Given the starting point and connectivities, the cascade extent could be found in each stochastic realization by solving the maximum flow problem: connect all nodes to a special target node t with edges of capacity = 1. and assign capacities $|V|E_{ij}$ to all i, j pairs. On this network, the maximal $s - t$ flow numerically equals the set of nodes affected by the cascade that originated in s . The latter term, efficiency, could be computed by finding the all-pairs distances in the graph defined by $E_{ij} = 1$, by solving a linear program for every pair. It would be advantageous to use an efficiency function that depends linearly on distances, if possible, rather than the non-linear definition in (2.2) above.

2.4.3 Computational Implementation

To investigate the cascade-resilience of dark networks, we used computational methods described in this section. We considered networks on $n = 180$ nodes constructed through 6 simple designs, chosen both based on empirical findings (see e.g.[2, 13]) as well as the possibility of analytic tractability in some cases. When more data becomes available on dark networks, it will become possible to extract additional subgraphs with statistical validity.

Three of the designs are based on identical “cells”: each cell is either (a) a clique (a complete graph), (b) a star (with a central node called “leader”), and (c) a cycle (nodes connected in a ring). Each of these have a single parameter, k – the number of nodes in the cell. Recent research suggests that under certain assumptions constructing networks from identical cells is optimal [27]. Let us also consider n -node graphs consisting of (d) randomly-connected cliques (sometimes termed “cavemen”), and (e) randomly-connected stars, in both cases according to probability p . Consider also (f) the simpler and well-studied Erdos–Renyi (ER) random graph with probability p (see figure in main text). By considering different structures for the cells we determine which of those structures provides the best performance.

The solution to the optimization problem is found by setting each of the parameters k (and when possible p) to various values. Each design D has “configurations” C_1^D, C_2^D, \dots each specifying the values of the parameters. Each configuration C_i^D is inputted to a program that generates an ensemble of 1 – 10 networks, whose average performance provides an estimate of the fitness of C_i^D . The number of networks was ten for networks with parameter p because there is higher variability between instances. The coefficient of variation (CV) in the fitness of the sample networks was monitored to ensure that the average is a reliable measure of performance. Typically CV was < 0.2 except near phase transitions of connectivity and percolation.

Optimization was performed using grid search. Alternative methods (e.g. Nelder–Mead) were considered but grid search was chosen despite its computational cost because it suffers no convergence problems even in the presence of noise (present due to variations in topology and contagion extent), and collects data useful for

sensitivity analysis and multi-objective optimization. The sampling grid was as follows. In designs consisting of cells of size k , cell size was set to all integer values in $[1, 180]$. If k did not divide 180, a cell of size $< k$ was added to ensure that the number of nodes in the graph is 180. The number of nodes is 180 because 180 is a highly-composite number and so it offers many networks of equally-sized cells. In general, normalization by n in the definitions of resilience and efficiency ensures that even when the number of nodes is tripled the effect of network size on fitness is very small for the above designs (around ± 0.05 in numerical experiments). In designs containing a parameter of connectivity p , it was set to all multiples of 0.05 in $[0, 1]$, with some extra points added to better sample phase transitions. The grid search algorithm results are readily used to compute the Pareto frontier using the ϵ -balls method [45] ($\epsilon = 0.01$).

The resilience metric is most easily computed by simulation where a node is selected at random to be “infected,” and the simulation is run until all nodes are in states S or R , and none is in state I . In the simplest version of the SIR cascade model, which we adopt, each node in the graph can be in one of three states “susceptible,” “infected” and “removed” designated S, I , and R , respectively (these names are borrowed from Epidemiology). Time is described in uniform discrete steps. A node in S state at time t stays in this state, unless a neighbor “infects” the node, causing it to move to state I at time $t + 1$. Specifically, a node in state S at time t has probability τ of turning to I state at time $t + 1$ for each adjacent node in state I at time t . Finally, a node in I state at time t always becomes R at time $t + 1$. Once in state R , the node remains there for all future times. It is possible to consider an alternate model where the rate of transition $I \rightarrow R$ takes more than one time step, but adding this effect would mostly serve to increase the probability of transmission, which is already parametrized by τ [57, 61].

A cascade/contagion that starts at a single node would run for up to n steps, but usually much fewer since typically $\tau < 1$ and/or the graph is not connected. To achieve good estimate of the average extent, the procedure was replicated 40 times, and then continued as long as necessary to achieve an error of under ± 0.5 node with a 95% confidence interval [46].

An analytic computation of the cascade extent metric was investigated. It is possible in theory because the contagion is a Markov process with states in the superset of the set of nodes, 3^n . Unfortunately, such a state space is impractically large. When G is a tree, then an analytic expression exists,¹ and it might be feasible when the treewidth is small [17, 57]. However, for many graph designs the tree approximation is not suitable. Another possible approach is to represent the contagion approximately as a system of differential equations which can be integrated numerically [39]. These possibilities were not pursued since the simulation approach could be applied to all graphs, while the errors of the analytic approaches are possibly quite large.

¹Specifically, the mean contagion size is $1 + \frac{pG'_0(1)}{1-pG'_1(1)}$, where $G_0(x)$ generates the degree distribution and $G_1(x) = \frac{G'_0(x)}{G_0(1)}$ generates the probability of arrival to a node [57].

2.5 Topological Cascade Resilience in the SIR-Reach Model

In this section and the rest of the paper, we will use the SIR-Reach model (R and W follow (2.1), (2.2)) The two models are attractive because they have real applications: Social Networks and Epidemiology. They have also been extensively explored by network scientists, which make them ideal as a case study in topological cascade resilience.

2.5.1 Optimal Network

The first set of experiments compares the designs against each other under different cascade risks (τ), Fig. 2.6. At each setting of τ , each design is optimized to its best configuration, i.e. the best cell size, and connectivity if applicable. The curves indicate the fitness of the optimal network in each design. Typically, at each τ the optimal network is different from the optimal network at another τ . Observe that within each design, as τ increases the fitness decreases – one cannot win when fighting cascades, only delay (see [30] for the proof). In certain applications, it

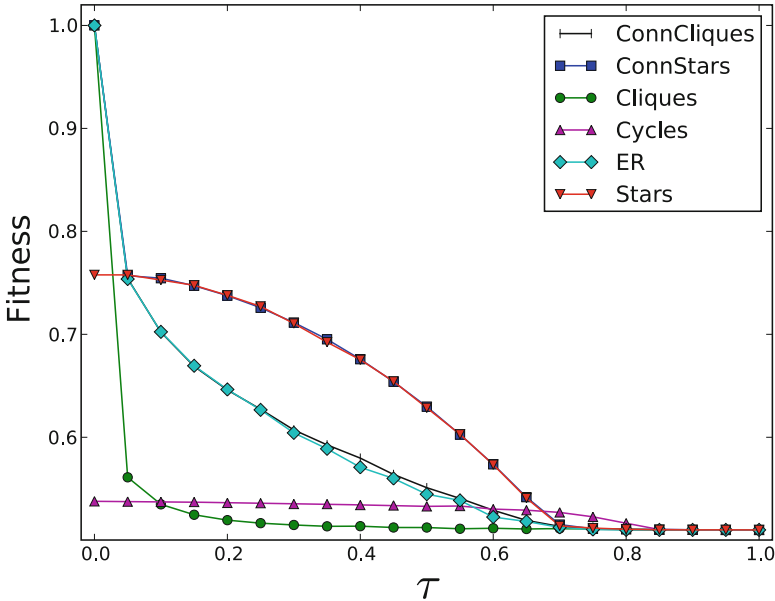


Fig. 2.6 Fitness at $r = 0.51$ of various network designs. The *Connected Stars* design is the best design at all cascade risks, τ . *Cliques* and *Connected Cliques* are competitive only for extreme ranges of τ . The superiority of *Connected Stars* over the ER (random graph) confirms the hypothesis that cells give fitness gains against cascades. The fitness of a design at each value of τ is defined as the fitness of the optimal configuration (network ensemble) within that design

is possible to invest in reducing the cascade propagation probability, τ . Then the curves in Fig. 2.6 could also be viewed as expressing the gain from efforts to reduce cascades by reducing τ and also adapting the network structure. If the slope is steep, then the gains are large.

Comparing designs to each other reveals that Connected Stars is superior to all others in fitness (Fig. 2.6). The design also outperforms any of the empirical networks in Fig. 2.2 in part because for each value of τ we selected the optimal network. The simpler Stars design is almost as fit, deteriorating only at extreme ranges of τ . The rankings of the designs are of course dependent on the parameter values, but not strongly (see [30] for the proof). Star-like designs are successful because the central node in a star acts as a cascade blocker while keeping the average distance in the star short (~ 2). Only for sufficiently low r , the Cliques, Connected Cliques and Connected Stars designs are superior to the Stars design. For such values of r efficiency is the dominant contributor to fitness. High weighting for efficiency benefits the former designs where efficiency can be 1 by constructing a fully connected (complete) graph. In the star design, efficiency is lower, reaching $\sim 1/2$ (when all nodes are placed in a single large star).

It has been long conjectured that cells provide dark networks with high resilience. Indeed, this is probably the reason why we found that dark networks have higher fitnesses than other networks. But cells also reduce the efficiency of a network since they isolate nodes from each other. To rigorously determine the net effect of cells, we compare the ER design (random graphs) to the Connected Stars design. ER is a strict subset of Connected Stars but only Connected Stars has cells. Therefore it is notable that Connected Stars has a higher fitness than ER, often significantly so. Indeed, cells must be the cause of higher fitness because cells are the only feature in Connected Stars that ER lacks.

2.5.2 Properties of Optimal Networks

Many properties of the optimal networks such as resilience, efficiency and edge density show rapid phase transitions as r is changed. For example, in the Cliques design when $r < 0.5$ the optimal network has high density that maximizes efficiency, whereas for $r > 0.5$ it is sparse and maximizes resilience (Fig. 2.7).

Intuition may suggest that the networks grow more sparse as cascade risk grows. Instead, the trend was non-monotonic (Fig. 2.7). For $\tau \gg 0$ and $r < 0.5$ Cliques, Connected Cliques, and Connected Stars became denser, instead of sparser, and for them the most sparse networks were formed in the intermediate values of τ where the optimal networks achieve both relatively high resilience and high efficiency. At higher τ values, when $r < 0.5$ it pays to sacrifice resilience because fitness is increased when efficiency is made larger through an equal or lesser sacrifice in resilience. The Stars design does not show a transition at $r = 0.5$ because it is hard to increase efficiency with this design.

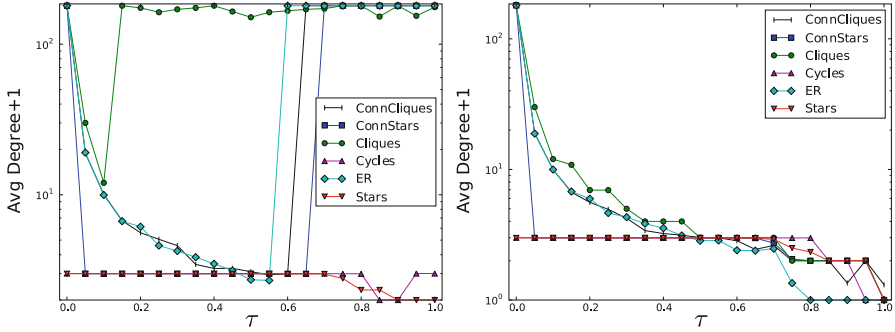


Fig. 2.7 Average degree in the optimal configuration of each design. At $r = 0.49$ (a) the optimization prefers networks that have high efficiency while at $r = 0.51$ (b) the preference is for resilience. In (b) the average degree diminishes monotonically to compensate for increasing cascade risk. In (a) most designs have a threshold τ at which they jump back to a completely-connected graph because structural cascade resilience becomes too expensive in terms of efficiency

2.5.3 Multi-objective Optimization

A complementary perspective on each design is found from its Pareto frontier of resilience and efficiency (Fig. 2.8). Typically a design is dominant in a part of the Resilience–Efficiency plane but not all of it. The Stars and Connected Stars designs can access most of the high resilience-low efficiency region. In contrast, the Cliques and Connected Cliques can make networks in the medium resilience-high efficiency regions.

The sharp phase transitions discussed earlier are seen clearly: along most of the frontiers, if we trace a point while decreasing resilience, there is a threshold at which a small sacrifice in resilience gives a major gain of efficiency. More generally, consider the points where the frontier is smooth. By taking two nearby networks on the frontier one can define a rate of change of efficiency with respect to resilience: $|\Delta W / \Delta R|$. The ratio can be used to optimize the network without using the parameter r . When $|\Delta W / \Delta R| \gg 1$ the network optimizer should choose to reduce to the resilience of the network in order to achieve great gains in efficiency; when $|\Delta W / \Delta R| \ll 1$ efficiency should be sacrificed to improve resilience.

2.6 Discussion

The analysis above considered both empirical networks and synthetic ones. The latter were constructed to achieve structural cascade resilience and efficiency. In contrast, in many empirical networks the structure emerges through an unplanned growth process or results from optimization to factors such as cost rather than blocking cascades. Without exception the synthetic networks showed higher fitness values

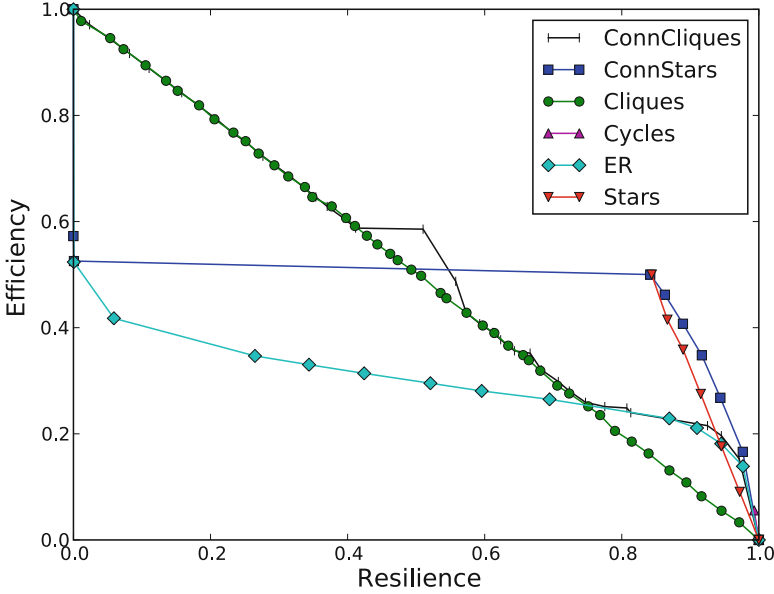


Fig. 2.8 The Pareto frontiers of various network designs ($\tau = 0.4$). The configurations of the *Connected Stars* design dominate over other designs when the network must achieve high resilience. However, designs based on *cliques* are dominant when high efficiency is required. Several designs show sharp transitions where at a small sacrifice of efficiency it is possible to achieve large increases in cascade resilience

despite the fact that they were based on very simple designs. This suggests that network optimization can significantly improve the fitness and cascade resilience of networks. It follows that an optimization process can be applied to design a variety of networks and to protect existing networks from cascades.

Many empirical networks also have power-law degree distributions [58]. Unfortunately, this feature significantly diminishes their cascade resilience: the resulting high-degree hubs make the networks extremely vulnerable to cascades once τ is slightly larger than 0 [20, 62].

In some successful synthetic networks, the density of edges increased when the cascade risk τ was high. This phenomenon has interesting parallels in non-violent social movements which are often organized openly rather than as secret underground cells even under conditions of severe state repression [70]. This openness greatly facilitates recruitment and advocacy, justifying the additional risk to the participants, just like the sacrifice of resilience to gain higher efficiency is justified under $r < 0.5$ conditions.

There are other important applications of this work, such as the design of power distribution systems. For power networks, the definition of resilience and efficiency will need to be changed. It would also be necessary to use much broader designs and optimization under design constraints such as cost. Furthermore, this work could also be adapted to domains of increasing concern such as financial credit networks, whose structure may make them vulnerable to bankruptcies [8, 36].

Acknowledgements This work has benefited from discussions with Aaron Clauset, Michael Genkin, Vadas Gintautas, Shane Henderson, Jason Johnson, and Roy Lindelauf, and anonymous reviewers. This paper extends the analysis originally published in [30]. Part of this work was funded by the Department of Energy at the Los Alamos National Laboratory (LA-UR 10-08349) under contract DE-AC52-06NA25396 through the Laboratory Directed Research and Development program, and by the Defense Threat Reduction Agency.

References

1. Albert, R., Jeong, H., Barabasi, A.L.: Error and attack tolerance of complex networks. *Nature (London)* **406**, 378–381 (2001)
2. Arquilla, J., Ronfeld, D.: *Networks and Netwars: The Future of Terror, Crime, and Militancy*. RAND Corporation, Santa Monica, CA (2001)
3. Ash, J., Newth, D.: Optimizing complex networks for resilience against cascading failure. *Physica A: Statistical Mechanics and its Applications* **380**, 673–683 (2007). DOI 10.1016/j.physa.2006.12.058
4. Baccara, M., Bar-Isaac, H.: How to organize crime. *Review of Economic Studies* **75**(4), 1039–1067 (2008)
5. Baker, W.E., Faulkner, R.R.: The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review* **58**(6), 837–860 (1993)
6. Ball, M.O.: Computing Network Reliability. *Operations Research* **27**(4), 823–838 (1979). DOI 10.1287/opre.27.4.823
7. Ball, M.O., Colbourn, C.J., Provan, J.S.: Network reliability. Tech. Rep. TR 1992-74, University of Maryland (1992)
8. Battiston, S., Gatti, D.D., Gallegati, M., Greenwald, B., Stiglitz, J.E.: Credit chains and bankruptcy propagation in production networks. *Journal of Economic Dynamics and Control* **31**, 2061–2084 (2007)
9. Briscoe, B., Odlyzko, A., Tilly, B.: Metcalfe’s law is wrong. *IEEE Spectrum* (2006)
10. Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O’Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A., von Winterfeldt, D.: A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* **19**(4), 733–752 (2003). DOI 10.1193/1.1623497
11. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. *Nature* **464**(7291), 1025–1028 (2010). DOI 10.1038/nature08932
12. Callaway, D.S., Newman, M.E.J., Strogatz, S.H., Watts, D.J.: Network robustness and fragility: Percolation on random graphs. *Phys. Rev. Lett.* **85**(25), 5468–5471 (2000). DOI 10.1103/PhysRevLett.85.5468
13. Carley, K.M.: Destabilization of covert networks. *Comput Math Organiz Theor* **12**, 51–66 (2006)
14. Centola, D., Macy, M.: Complex contagions and the weakness of long ties. *American J. Sociology* **113**(3), 702–734 (2007)
15. Cohen, R., Erez, K., ben Avraham, D., Havlin, S.: Resilience of the internet to random breakdowns. *Phys. Rev. Lett.* **85**(21), 4626–4628 (2000). DOI 10.1103/PhysRevLett.85.4626
16. Colbourn, C.J.: Network resilience. *SIAM Journal on Algebraic and Discrete Methods* **8**(3), 404–409 (1987). DOI 10.1137/0608033
17. Colcombet, T.: On families of graphs having a decidable first order theory with reachability. In: P. Widmayer, S. Eidenbenz, F. Triguero, R. Morales, R. Conejo, M. Hennessy (eds.) *Automata, Languages and Programming, Lecture Notes in Computer Science*, vol. 2380, pp. 787–787. Springer Berlin / Heidelberg (2002)
18. Conn, A.R., Scheinberg, K., Vicente, L.N.: *Introduction to Derivative-Free Optimization*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA (2009)

19. Cowie, J.H., Ogielski, A.T., Premore, B., Smith, E.A., Underwood, T.: Impact of the 2003 blackouts on internet communications: Preliminary report. Tech. rep., Renesys Corporation (2004). www.renesys.com
20. Crepey, P., Alvarez, F.P., Barthelemy, M.: Epidemic variability in complex networks. *Physical Review E (Statistical, Nonlinear, and Soft Matter Physics)* **73**(4), 046131 (2006). DOI 10.1103/PhysRevE.73.046131
21. Crucitti, P., Latora, V., Marchiori, M.: Model for cascading failures in complex networks. *Phys. Rev. E* **69**(4), 045104 (2004). DOI 10.1103/PhysRevE.69.045104
22. Dobson, I., Carreras, B.A., Lynch, V.E., Newman, D.E.: Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science* **17**(2), 026103 (2007). DOI 10.1063/1.2737822
23. Doyle, J.C., Alderson, D.L., Li, L., Low, S., Roughan, M., Shalunov, S., Tanaka, R., Willinger, W.: The "robust yet fragile" nature of the Internet. *Proceedings of the National Academy of Sciences* **102**(41), 14,497–14,502 (2005). DOI 10.1073/pnas.0501426102
24. Draief, M., Ganesh, A., Massoulié, L.: Thresholds for virus spread on networks. *Annals of Applied Probability* **18**(2), 359–378 (2008). DOI 10.1214/07-AAP470
25. Finbow, A.S., Hartnell, B.L.: On designing a network to defend against random attacks of radius two. *Networks* **19**(7), 771–792 (1989). DOI 10.1002/net.3230190704
26. Gleeson, J.P., Cahalane, D.J.: Seed size strongly affects cascades on random networks. *Phys. Rev. E* **75**(5), 056103 (2007). DOI 10.1103/PhysRevE.75.056103
27. Goyal, S., Vigier, A.: Robust networks (2010). Working paper <http://sticerd.lse.ac.uk/seminarpapers/et11032010.pdf>
28. Guimerà, R., Danon, L., Díaz-Guilera, A., Giralt, F., Arenas, A.: Self-similar community structure in a network of human interactions. *Phys. Rev. E* **68**(6), 065103 (2003). DOI 10.1103/PhysRevE.68.065103
29. Gunther, G., Hartnell, B.L.: On minimizing the effects of betrayals in resistance movements. In: *Proceedings of the Eighth Manitoba conference on Numerical Mathematics and Computing*, pp. 285–306 (1978)
30. Gutfraind, A.: Optimizing topological cascade resilience based on the structure of terrorist networks. *PLoS ONE* **5**(11), e13448 (2010). DOI 10.1371/journal.pone.0013448
31. Gutfraind, A.: Monotonic and Non-Monotonic Epidemiological Models on Networks. <http://arxiv.org/abs/1005.3470>
32. Hartnell, B.L.: The optimum defense against random subversions in a network. In: *Proceedings of the Tenth Southeast conference on Combinatorics Graph Theory and Computing*, pp. 494–499 (1979)
33. Holme, P.: Efficient local strategies for vaccination and network attack. *Europhys. Lett.* **68**(6), 908–914 (2004)
34. Holme, P., Kim, B.J., Yoon, C.N., Han, S.K.: Attack vulnerability of complex networks. *Phys. Rev. E* **65**(5), 056109 (2002). DOI 10.1103/PhysRevE.65.056109
35. Huang, W., Li, C.: Epidemic spreading in scale-free networks with community structure. *J Stat Mech* **P01014** (2007)
36. Iori, G., Masi, G.D., Precup, O.V., Gabbi, G., Caldarelli, G.: A network analysis of the italian overnight money market. *Journal of Economic Dynamics and Control* **32**, 259–278 (2008)
37. J. Leskovec, J.K., Faloutsos, C.: Graph Evolution: Densification and Shrinking Diameters. *ACM Transactions on Knowledge Discovery from Data (ACM TKDD)* **1**(1) (2007)
38. Johnson, J.K., Chertkov, M.: A majorization-minimization approach to design of power transmission networks. In: *Proceedings of the 49th IEEE Conference on Decision and Control (CDC '10)* (2010)
39. Keeling, M.J.: The effects of local spatial structure on epidemiological invasions. *Proc R Soc Lond B* **266**, 859–867 (1999)
40. Kempe, D., Kleinberg, J., Tardos, E.: Maximizing the spread of influence through a social network. In: *KDD '03: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 137–146. ACM, New York, NY, USA (2003)
41. Klau, G.W., Weiskircher, R.: Robustness and resilience. In: *Network Analysis, Lecture Notes in Computer Science* 3418, pp. 417–437. Springer-Verlag (2005)

42. Krebs, V.E.: Mapping networks of terrorist cells. *Connections* **24**(3), 43–52 (2002)
43. Lai, Y.C., Motter, A., Nishikawa, T.: Attacks and cascades in complex networks. In: *Complex Networks: Lecture Notes in Physics* 650, pp. 299–310. Springer-Verlag (2004)
44. Latora, V., Marchiori, M.: Efficient behavior of small-world networks. *Phys. Rev. Lett.* **87**(19), 198,701 (2001). DOI 10.1103/PhysRevLett.87.198701
45. Laumanns, M., Thiele, L., Deb, K., Zitzler, E.: Combining convergence and diversity in evolutionary multiobjective optimization. *Evolutionary Computation* **10**(3), 263–282 (2002). DOI 10.1162/106365602760234108. PMID: 12227996
46. Law, A., Kelton, W.D.: *Simulation Modeling and Analysis*, 3 edn. McGraw-Hill Higher Education, New York (1999)
47. Leskovec, J., Kleinberg, J.M., Faloutsos, C.: Graphs over time: densification laws, shrinking diameters and possible explanations. In: *KDD*, pp. 177–187 (2005)
48. Lindelauf, R.H., Borm, P.E., Hamers, H.: On Heterogeneous Covert Networks. SSRN eLibrary (2008)
49. Lindelauf, R.H., Borm, P.E., Hamers, H.: The Influence of Secrecy on the Communication Structure of Covert Networks. *Social Networks* **31**(2) (2009)
50. Marler, R., Arora, J.: Survey of multi-objective optimization methods for engineering. *Structural and Multidisciplinary Optimization* **26**, 369–395(27) (April 2004). DOI doi:10.1007/s00158-003-0368-6
51. Miksche, F.O.: *Secret Forces*, 1st edn. Faber and Faber, London, UK (1950)
52. Morselli, C., Petit, K., Giguere, C.: The Efficiency/Security Trade-off in Criminal Networks. *Social Networks* **29**(1), 143–153 (2007)
53. Motter, A.E.: Cascade control and defense in complex networks. *Phys. Rev. Lett.* **93**(9), 098,701 (2004). DOI 10.1103/PhysRevLett.93.098701
54. Motter, A.E., Lai, Y.C.: Cascade-based attacks on complex networks. *Phys. Rev. E* **66**(6), 065,102 (2002). DOI 10.1103/PhysRevE.66.065102
55. Motter, A.E., Nishikawa, T., Lai, Y.C.: Range-based attack on links in scale-free networks: Are long-range links responsible for the small-world phenomenon? *Phys. Rev. E* **66**(6), 065,103 (2002). DOI 10.1103/PhysRevE.66.065103
56. Mueller-Gritschneider, D., Graeb, H., Schlichtmann, U.: A successive approach to compute the bounded pareto front of practical multiobjective optimization problems. *SIAM Journal on Optimization* **20**(2), 915–934 (2009). DOI 10.1137/080729013
57. Newman, M.E.J.: Spread of epidemic disease on networks. *Phys. Rev. E* **66**(1), 016,128 (2002). DOI 10.1103/PhysRevE.66.016128
58. Newman, M.E.J.: The structure and function of complex networks. *SIAM Review* **45**(2), 167–256 (2003). DOI 10.1137/S003614450342480
59. Newman, M.E.J.: Finding community structure in networks using the eigenvectors of matrices. *Phys. Rev. E* **74**(3), 036,104 (2006). DOI 10.1103/PhysRevE.74.036104
60. Newman, M.E.J., Forrest, S., Balthrop, J.: Email networks and the spread of computer viruses. *Phys. Rev. E* **66**(3), 035,101 (2002). DOI 10.1103/PhysRevE.66.035101
61. Noël, P.A., Davoudi, B., Brunham, R.C., Dubé, L.J., Pourbohloul, B.: Time evolution of epidemic disease on finite and infinite networks. *Phys. Rev. E* **79**(2), 026,101 (2009). DOI 10.1103/PhysRevE.79.026101
62. Pastor-Sarorras, R., Vespignani, A.: Epidemic spreading in scale-free networks. *Phys Rev Lett* **86**(14), 3200–3203 (2001)
63. Phadke, A., Thorp, J.: Expose hidden failures to prevent cascading outages [in power systems]. *Computer Applications in Power*, IEEE **9**(3), 20–23 (1996). DOI 10.1109/67.526849
64. Pourbohloul, B., Meyers, L., Skowronski, D., Krajden, M., Patrick, D., Brunham, R.: Modeling control strategies of respiratory pathogens. *Emerg. Infect. Dis.* **11**(8), 1246–56 (2005)
65. Raab, J., Milward, H.B.: Dark Networks as Problems. *J Public Adm Res Theory* **13**(4), 413–439 (2003). DOI 10.1093/jopart/mug029
66. Ripeanu, M., Foster, I., Iamnitchi, A.: Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design. *IEEE Internet Computing Journal* **6**(1) (2002)

67. Rodriguez, J.: The march 11th terrorist network: In its weakness lies its strength (2004). Working Papers EPP-LEA, University of Barcelona
68. Ron, D., Safro, I., Brandt, A.: Relaxation-based coarsening and multiscale graph organization. SIAM Multiscale Modeling and Simulations (under revision) (2010). Preprint ANL/MCS-P1696-1009
69. Sageman, M.: Leaderless Jihad - Terror Networks in the Twenty-First Century. University of Pennsylvania Press, Philadelphia, PA (2008)
70. Sharp, G.: From dictatorship to democracy: A conceptual framework for liberation. The Albert Einstein Institution, East Boston, Massachusetts (2003)
71. U.S. Government: The 9/11 Commission Report. US Government Printing Office, Washington, DC (2007)
72. Watts, D.J.: A simple model of global cascades on random networks. Proceedings of the National Academy of Sciences of the United States of America **99**(9), 5766–5771 (2002). DOI 10.1073/pnas.082090499
73. Woo, G.: Mathematical Methods in Counterterrorism, chap. Intelligence Constraints on Terrorist Network Plots, pp. 205–214. Springer-Verlag (2009). Nasrullah Memon and Jonathan D. Farley and David L. Hicks and Torben Rosenorn, Eds.
74. Zawodny, J.: Internal organization problems and the sources of tensions of terrorist movements as catalysts of violence. Terrorism: An International Journal (continued as Studies in Conflict and Terrorism) **1**(3/4), 277–285 (1978)
75. Zhang, Y., Prica, M., Ilic, M., Tonguz, O.: Toward smarter current relays for power grids. In: Power Engineering Society General Meeting, 2006. IEEE, p. 8 (2006). DOI 10.1109/PES.2006.1709580

Handbook of Optimization in Complex Networks

Communication and Social Networks

Thai, M.T.; Pardalos, P. (Eds.)

2012, XII, 544 p., Hardcover

ISBN: 978-1-4614-0856-7