Modeling, Analysis, and Optimization of Robustness in Interdependent Networks against Cascading Failures

Submitted in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy
in
Electrical and Computer Engineering

Yingrui Zhang

B.Eng. Electronic and Communication Engineering
Beijing University of Posts and Telecommunications, Beijing, China

M.Phil. Electronic and Computer Engineering
Peking University, Beijing, China

Carnegie Mellon University
Pittsburgh, PA

May, 2019

For Yichen and Jonathan.

Thesis Committee Members

Prof. Osman Yağan (Advisor)
Department of Electrical and Computer Engineering
Carnegie Mellon University

Prof. Bruno Sinopoli
Department of Electrical and Computer Engineering
Carnegie Mellon University

Prof. Filippo Radicchi
Center for Complex Networks and Systems Research
School of Informatics and Computing
Indiana University

Sila Kiliccote
SLAC National Accelerator Laboratory
Precourt Institute for Energy
Stanford University

Abstract

Critical infrastructures, including those that concern the nation's economy and security such as electrical power systems, water distribution systems and transportation systems, are becoming more and more interdependent with each other. Although they bring unprecedented improvements on efficiency and flexibility, the interdependent relations enable failures in one network to propagate and impact the performance of other coupled networks. Cascading failures is one such phenomenon that creates dramatic damages to critical infrastructures, where a small initial shock can get escalated due to the intricate dependencies and result in system-wide collapses. This dissertation aims to understand and mitigate the root cause of the seemingly unexpected large-scale cascading failures by characterizing and modeling the inherent dependencies between and within different networks. A main finding is that allocating the available redundancies *uniformly* across the system maximizes the robustness against random failures.

We support this thesis statement with different networks and attack types: flow-carrying networks under random and targeted attack, interdependent flow-carrying networks under random attacks, and interdependent cyber-physical networks under random attacks. In the flow redistribution network, we propose a global and equal flow redistribution model to capture the cascading failure dynamics. In the case of random attacks, we derive the final system size and critical attack size, and prove that the optimal robustness is reached when system redundancy is allocated uniformly. For targeted attacks, we propose the optimization problem of finding the best k lines to attack so as to minimize the number of alive lines at the steady-state, to reveal the worst-case attack vulnerability of the system. In interdependent flow-carrying networks, we study a model where the flow of a failed line is redistributed partially within the network that the failed line belongs to, with the rest being shed to other coupled networks. Analyzing the cascading failures in this model, we show that interdependence has a multi-faceted impact on system robustness in that as the level of coupling increases, the chance for both networks to survive or collapse concurrently increases, whereas it becomes more difficult

for each component network to survive on its own. To understand the robustness of integrated cyber-physical systems (CPSs), we develop a novel interdependent system model to capture the inherently different failure cascade characteristics of each component network; i.e., the cyber and the physical networks are governed by different cascade rules to be able to function. We demonstrate the ability of our model to capture the unexpected nature of large-scale cascading failures in CPSs, and provide insights on improving system robustness by proposing optimal redundancy allocation schemes.

Acknowledgements

Being a member of Carnegie Mellon University and spending four years here pursing the PhD degree has been one of the most memorable of my life. The PhD training has granted me the ability of independent thinking, questioning, doing research and digging for answers; while the life in CMU teaches me how to survive in a highly competitive environment and strive for the best. When I look back, besides the degree and published papers, I'm really grateful for the people that walk this way with me. First and foremost, I would like to thank my advisor Prof. Osman Yağan, without whom none of this would happen, for being an excellent role model in research that I learn so much from, a nice mentor that lead my way in research and give me the freedom to explore, and a considerate friend during the difficulties in life. Thank you Prof. Yağan!

I would also like to thank Prof. Bruno Sinopoli, Prof. Filippo Radicchi and Sila Kiliccote for serving my thesis committee. Their valuable feedback for the past year help me to be more rigorous and precise, and to look research problems from different perspectives. My PhD research was supported by the National Science Foundation project "Robust and Optimal Design of Interdependent Networks"(CCF #1422165), and I'm also thankful to Prof. Alex Arenas for his support and help in the work of interdependent flow-carrying networks. I want to thank my collaborator Vaggos Chatziafratis and Dr. Talha Cihad Gulcu on the work of attack vulnerability of flow-carrying networks, and I'm really grateful to Prof. Tze Meng Low for helping me speedup the simulations as well as the discussions on some concepts.

I want to thank the members of our group, Rashad Eletreby, Yong Zhuang, Mansi Sood, Samarth Gupta, for the discussions and feedbacks on my work, as well as all the support and encouragement from them. I would also like to thank the A-level dwellers of Hamerschlag Hall, Jiyuan Zhang, Guanglin Xu, Doru Thom Popovici, Zhipeng Zhao, for the tears and laughter we shared during the years of PhD life. I want to thank the members of the Agape life church in Pittsburgh, who gave me great support spiritually and in life when I struggle, the Brian-

Kim Woo family, Preethi Josephina, Genna Frederick, Allison Oguh, William Bishop, Adeline Giritharan, Su Tsai, and all others that generously and kindly spent their time helping me and encouraging me.

Last but not least, I am deeply grateful to our Heavenly Father, Lord Jesus, for supplying all the needs, and give me a great advisor, wonderful friends and family for my life. I thank the love and support from my husband Yichen, who took care of our son during my defense and is always there with me, as well as my parents and in-laws who support my way through the PhD. This thesis is dedicated to them with my sincere gratitude.

Contents

List of Figures

List of Tables

Part I

Introduction and Background

Chapter 1

Introduction and Motivation

Our national security, economic prosperity, and national well-being are dependent upon a set of highly interdependent critical infrastructures, examples include the national electrical grid, oil and natural gas systems, telecommunication and information networks, transportation networks, water systems, and banking and financial systems. However, while the interdependent relations bring unprecedented improvements and functionality to the critical infrastructures as well as improve the economy, it has been observed that such interdependent systems tend to be fragile against failures, natural hazards, and attacks [7]. For instance, in the event of an attack or random failures in an interdependent system, the failures in one network can cause failures of the dependent nodes in other coupled networks and vice versa. This process may continue in a recursive manner, triggering a cascade of failures that can potentially collapse an entire system. For instance, an adversarial attack to any essential Internet hosts, e.g., tier-1 ISPs such as Qwest, AT&T or Sprint servers, once successful, may cause tremendous breakdowns to both millions of online services and the further large-area blackout because of the cascading failures [8]. As we can see, the failures in these interdependent networks are far more complicated and destructive than the failures in an isolated network, because the systems are exposed to threats not only to themselves but also to the cascading failures induced by their interdependent systems. The smart grid is such an example, where the power grid network and the information network are coupled together; the grid depends on the information network for its control, and the information network depends on the grid for power. In fact, the cascading effect of even a partial Internet blackout could disrupt major national infrastruc-

ture networks involving Internet services, power grids and financial markets [9]. For example, it was shown [10] that the electrical blackout that affected much of Italy on 28 September 2003 had started with the shutdown of a power station, which led to failures in the Internet communication network, which in turn caused the breakdown of more stations, and so on.

Given the importance of their reliable and secure operations, understanding the behavior of these infrastructures – particularly when stressed or under attack – is crucial. As we embark on a future where interdependent systems are becoming an integral part of our daily lives, a fundamental question arises as to how we can design them in a *robust* and *reliable* manner. Numerous applications of interdependent systems – including those that concern the nation's security, the health care system, monitoring and protecting natural landscapes, the electrical power system, and emergency services – clearly put the successful and efficient operation of them at the core of technologies that are vital to us. To that end, a major focus has to be put on understanding their vulnerabilities, and in particular the root cause of the seemingly unexpected but large scale cascading failures through an accurate characterization and modeling of these inherent dependencies.

Models and simulations can provide considerable insight into the complex nature of the behaviors and operational characteristics of the critical infrastructures, but they must include interdependent relations if they are to provide accurate representations of infrastructure characteristics and operations. Traditional network science falls short in providing such a characterization since the focus has mainly been on single networks in isolation; i.e., networks that do not interact with, or depend on any other network. The current literature on robustness of interdependent networks focus extensively on percolation-based models [9, 11–15], where a node can function only if it belongs to the largest connected (i.e., giant) component of its own network; nodes that lose their connection to this giant core are deemed *non-functional*. While such models are suitable for many cases such as information networks, they fail to accurately capture the dynamics of cascading failures in many real-world systems that are tasked with transporting physical commodities; e.g., power networks, traffic networks, etc. In such

flow-carrying networks, failure of nodes (or, lines) lead to *redistribution* of their load to functional nodes, potentially *overloading* and failing them. As a result, the dynamics of failures is governed primarily by load redistribution rather than the structural changes in the network. A real-world example to this phenomenon took place on July 21, 2012, when a heavy rain shut down a metro line and caused 100 bus routes to detour, dump stop, or stop operation completely in Beijing [16].

Another problems is, despite some recent research activity aimed at studying interdependent networks [9,17–21], very few consider engineering aspects of inter-dependent networks and very little is known as to how such systems can be designed to have maximum robustness under certain design constraints; see [22–25] for rare exceptions. The current literature is also lacking interdependent system models that enabling the study of robustness of systems that integrate networks with inherently different behavior, such as the fundamental difference between the *physical* and *cyber* networks in the cyber-physical systems; e.g., the functionality of the physical subsystem would be primarily governed by the physical flows and capacities associated with its components, while in a cyber-network, system-wide connectivity would be the prominent requirement for maintaining functionality. There is thus a need to develop new approaches for modeling and analyzing cascading failures in interdependent systems, and considering engineering aspect of improving the robustness of interdependent networks. This dissertation aims to solve the abovementioned problems by accurately characterize and model the inherent dependencies between and within different networks in interdependent systems. With our approach, we make an effort to understand the root cause of the seemingly unexpected large-scale cascading failures that are able to create dramatic damages to critical infrastructures. We will also demonstrate through our analysis that, uniform redundancy allocation in the system maximizes robustness over all random failures sizes under a flow redistribution model.

1.1 Research theme and considered research problems

As we mentioned before, the study on robustness of networks has long been concentrated on the case of a single or isolated network which doesn't interact with other networks. However, this is rarely the case in our life and society now. Modern infrastructures are becoming significantly more dependent on each other, making a system more complicated with interacting networks involved. A fundamental property of interdependent networks is that failures happen in one network can propagate to another coupled network in the system, where the failure may bounce back and forth between the initial failed network and its coupled networks, causing a global cascade of failures. This type of failure will lead to a much severe damage, for example of failure of a power grid may cause failures in financial systems, water distribution systems, transportation systems and so on, potentially collapsing the functionality of the whole society. In this thesis, we aim to answer the question of how we can understand the vulnerabilities and further design interdependent infrastructure systems in a robust manner.

Understanding the vulnerabilities and the root cause of the seemingly unexpected large-scale cascading failures passes through accurately characterizing and modeling the inherent dependencies between and within different component networks. The studies of network topologies and degree distributions are quite extensive; see [26–30] for some examples. These models are often suitable for information or cyber networks, since the robustness of a network is justified by the largest connected component (i.e., giant component) based on percolation rules. In other words, a node in such networks needs to connect to the giant core in order to function. However, most of the percolation based models do not consider the real load or flow carried by the network, which is often the case in real-world. Actually, the literature falls short in characterizing networks carrying a physical flow or load. Especially, the different load redistribution rules upon failure has been understudied. This is an important module for interdependent networks, since in many real-world applications physical networks are substantial in maintaining the functionality of an interdependent system. Thus, we study the robustness of a flow-carrying

networks under an equal and global redistribution model, where when a node or a line fail, the load it carried will be redistributed equally among all the alive nodes (or lines). The proposed model takes into consideration the long-range effect in many systems, where failures not only affect neighboring regions, but also influence the load in far away areas in the system. This phenomenon is observed in many systems such as the power grid, and the proposed model is shown to capture this character of the system.

Under the equal and global redistribution model, we will study the robustness of a flow-carrying network initiated by both a *random* attack and a *targeted* attack. Random attacks model the random events that cause initial failure in the system such as urgent weather conditions, misoperation, etc. We will analyze the final system size, critical attack size above which the system completely collapses, and the transition behavior (how system transit from certain level of functionality to completely breakdown) against cascading failures started by randomly remove a portion of lines in the network. In the case of targeted attacks, we will study the optimization problem of finding the best k lines to attack so as to minimize the number of *alive* lines at the steady-state (i.e., when cascades stop). This is done to reveal the worst-case attack vulnerability of the system as well as to reveal its most vulnerable lines. We will furthermore consider a modified optimization problem where the adversary is also constrained by the *total* load (in addition to the number) of the initial attack set, and develop heuristic algorithms for both the original and modified problems.

In reality, networks with similar function are often coupled together to construct an interdependent structure for better robustness and lower risk, for example power networks of different region may be coupled together; or similar financial institutes may be related to lower system risk. We model this type of system as an interdependent networks composed of two identical networks under a flow redistribution model, and will investigate dynamics and behavior of the system during the cascading failure process. Due to the interdependent relations between component networks, load on failed lines (or nodes) will not only be redistributed internally, but will also be redistributed across other component networks. To quantify the

level of the interdependency, we will define coupling coefficients that represent the percentage of load shed from failure-initiated network to other networks. After redistribution of load from failed lines (or nodes), more failure will happen within the network and across the system, potentially leading to a cascade of failures in multiple component networks, till the system reaches a steady state and no more failures happen. We will analyze the cascading dynamics and system behavior during this process, and propose a resource allocation scheme to reach optimal robustness.

Turning from interdependent systems composed of similar function networks, next we consider interdependent systems composed of sub-networks of inherently different characters, a typical example is the cyber-physical systems (CPS). CPS are integration of computing and physical processes [31], and often in the real-world we have a physical network and cyber network for different processes. Due to the interdependent relations, usually the physical network affects the cyber network by providing a unique physical substance, and the cyber network sends out control and communication information without which the physical network cannot function. There are considerable challenges, particularly because the physical components of the CPS introduce safety and reliability requirements qualitatively different from those in general-purpose cyber networks [31]. Moreover, physical networks are qualitatively different from cyber networks, in a way that the failure is often caused by redistribution of load while the cyber networks rely more on the connectivity to the giant core. To this end, we will capture this fundamental difference between the two types of networks by proposing a framework with *inter-dependency* relations and *intra-dependency* relations defined. Specifically, *inter-dependency* relations define the rules and physical laws within each component network; and *intra-dependency* relations define the interdepend relations between coupled networks. The interdependent relations between component networks are established through one-to-one links, and we will provide a thorough analysis of the dynamics of cascading failures in this interdependent system initiated with a random attack.

Till now, we mainly focus on the study of a global redistribution rule when flow-carrying

networks are involved. In other words, loads will be redistributed globally to all alive lines upon failure. In this thesis, we also complement our results with simulations on a global-local combined redistribution model. In this model, a factor β controls how many load of the failed nodes goes to geographic neighbors, and how many goes to everyone else. We will explore different β values under this model, and analyze how topology brings changes as well as keeps qualitatively behaviors the same for different β values.

1.2 Thesis contributions

We pursue the study on modeling and analyzing the robustness of interdependent networks against cascading failures. Through accurately characterizing and modeling the inherent dependencies between and within component networks, we analyze and help to understand the root cause of the seemingly unexpected large-scale cascading failures. Furthermore, we show that uniform redundancy allocation in the system maximizes robustness over all random failures sizes.

Regarding the flow-carrying networks, we propose a global and equal redistribution model that takes into consideration the cascading failure effect caused by load redistribution. Our model captures the long-range effect existing in many systems, and we provide a complete understanding of system robustness under random attacks by i) deriving an expression for the final system size as a function of the size of initial attacks; ii) deriving the critical attack size after which system breaks down completely; iii) showing that complete system breakdown takes place through a first-order (i.e., discontinuous) transition in terms of the attack size; and iv) establishing the optimal load-capacity distribution that maximizes robustness. In the scenario of targeted attacks, we propose the *optimization* problem of finding the best k lines to attack so as to minimize the number of *alive* lines at the steady-state (i.e., when cascades stop). This reveals the worst-case attack vulnerability of the system as well as its most vulnerable lines. We derive optimal attack strategies in several special cases of load-capacity distributions that are practically relevant. We also prove the modified problem where the adversary is further

constrained by the *total* load (in addition to the number) of the initial attack set is NP-Hard. Besides the analysis, we develop heuristic algorithms for selecting the attack set for both the original and modified problems.

Then, we consider the case of interdependent networks under a flow-redistribution model. Specifically, we consider a model consisting of networks A and B with initial line loads and capacities. When a line fails in system A, a-fraction of its load is redistributed to alive lines in B, while remaining $(1-a)$-fraction is redistributed equally among all functional lines in A; a line failure in B is treated similarly with b giving the fraction to be redistributed to A. We give a thorough analysis of cascading failures of this model initiated by a random attack targeting p_1-fraction of lines in A and p_2-fraction in B. We show that the model captures the real-world phenomenon of unexpected large scale cascades and exhibits interesting transition behavior; network robustness tightly depends on the coupling coefficients a and b, and robustness is maximized at non-trivial a, b values in general. Unlike existing models, we show in our work that interdependency has a multi-faceted impact on system robustness in that it can lead to an improved robustness for each individual network.

For interdependent systems composed of networks with inherently different characters, we investigate the cascading failure dynamics and system robustness of a cyber-physical system, also initiated by a random attack. We develop a novel interdependent system model to capture the intricate dependencies within and across the individual (e.g., cyber and physical) counterparts of the system, with different failure rules in the cyber network and physical network. For simplicity, we consider a one-to-one interdependency model where every node in the cyber-network is dependent upon and supports a single node in the physical network, and vice versa. We provide a thorough analysis of the dynamics of cascading failures in this interdependent system initiated with a random attack. The system robustness is quantified as the *surviving* fraction of nodes at the end of cascading failures, and is derived in terms of all network parameters involved (e.g., degree distribution, load/capacity distribution, failure size, etc.). Among other things, these results demonstrate the ability of our model to capture the

unexpected nature of large-scale failures, and provide insights on improving system robustness.

For the global redistribution model studied in this thesis, we further complement our analytical results with simulations that demonstrate how network topology affects the robustness properties. To this end, we propose a model that combines the global redistribution model and the local redistribution model. We show that the qualitative behavior of the robustness remains relatively unchanged, and suggest that the mean-field approached used in our analysis is able to capture well the qualitative behavior of the final system size for different global-local parameters.

1.3 Thesis outline

This thesis is divided into four parts. In Part I, we introduce the motivation, research theme, research problems, research contributions, as well as the background for this thesis. In Part II, we consider the robustness of flow-carrying networks. In particular, we consider the cascading failures in flow-carrying networks initiated by a random attack (Chapter 3) and the case when targeted attack is deployed (Chapter 4). In Part III, we consider interdependent networks and their robustness behavior against cascading failures. We considered interdependent systems composed of similar networks and inherently different networks; specifically, the case of interdependent flow-carrying networks (similar networks coupled) introduced in Chapter 5 and cyber-physical systems (inherently different networks coupled) studied in Chapter 6. Finally, Part IV summarizes the conclusion and future work for this thesis.

1.4 Table of symbols used in the thesis

symbol	meaning	explanation
$1-p$	initial failure size	fraction of initially failed nodes (or line)
$\mathcal{L}_i$	line	a line in the network
L_i	initial load	initial load carried by line $\mathcal{L}_i$
S_i	free-space	redundancy available to line $\mathcal{L}_i$
C_i	capacity	maximum flow line $\mathcal{L}_i$ can sustain
α_i	tolerance factor	the proportion of L_i with C_i
$U(L_{min}, L_{max})$	Uniform distribution	$L_{min}, L_{max} > 0$
$Pareto(L_{min}, b)$	Pareto distribution (power-law distribution)	$L_{min}, b > 0$
$Weibull(L_{min}, \lambda, k_w)$	Weibull distribution	$L_{min}, \lambda, k_w > 0$
β	parameter in heuristic algorithm for targeted attacks	used in maximum $L * S^{\beta} attack$
k	attack size in targeted attacks	number of lines attacked initially
a, b	coupling coefficients	a (or b) fraction of load is shed to the coupled network; $1-a$ (or $1-b$) is shed within
$\langle d \rangle$	mean degree	mean degree in ER or SF graph
$SF(\gamma, \Gamma)$	scale-free network	power-law degree distribution with exponential cut-off; γ is the power exponent and Γ is the cut-off parameter
μ	parameter in global-local combined redistribution	μ fraction of load distributed to neighbors, the rest to all other functional lines or nodes

Table 1.1: Symbols used in the thesis and their meanings.

Chapter 2

Background

2.1 Cascading failures in critical infrastructures

Robustness and vulnerabilities of real world systems have always been an important issue, and due to the fast development of information technologies and the recent advances in complex network theory [32–37], networks now play an even more important role in modeling and analyzing system infrastructures that compose the basics of our lives and industry. Cascading failures are one of the most important issues studied in the robustness of various systems, since the breakdown of a single or a very small size group of elements can be sufficient to cause the entire systems to collapse, due to the dynamics of redistribution of flows on the networks [38]. How is it possible that a small initial shock, such as the breakdown of a node in the power system or a route in traffic system, can trigger avalanches affecting a considerable fraction of the system, or even collapsing a system that was proven to be stable with respect to similar shock in the past? In this thesis, we try to answer this question and aim to model and analyze the robustness of interdependent systems (or networks) regarding the cascading failure phenomenon.To take into account this phenomenon, we need to apply dynamical approaches due to the fact that the breakdown of a small region of the system not only affect the network performance directly, but also can cause an overload and consequently the breakdown of failure of other parts of the network, which may further cause failure in the redistribution process, thus generating a cascading effect that may collapse the entire network.

The most vital infrastructure where cascading failure can create huge damage is the elec-

blackout events	people affected (millions)	location	date
2012 India blackouts	620	India	30-31 Jul 2012
2001 India blackout	230	India	2 Jan 2001
2014 Bangladesh blackout	150	Bangladesh	1 Nov 2014
2015 Pakistan blackout	140	Pakistan	26 Jan 2015
2005 Java-Bali blackout	100	Indonesia	18 Aug 2005
1999 Southern Brazil blackout	97	Brazil	11 Mar-22 Jun 1999
2009 Brazil and Paraguay blackout	87	Brazil, Paraguay	10-17 Nov 2009
2015 Turkey blackout	70	Turkey	31 Mar 2015
Northeast blackout of 2003	55	United States, Canada	14-15 Aug 2003
2003 Italy blackout	55	Italy, Switzerland	28 Sept 2003
2016 Kenya Blackout	44	Kenya	7 Jun 2016
2002 Luzon blackout	40	Philippines	21 May 2002
1978 Thailand blackout	40	Thailand	18 Mar 1978
2001 Luzon blackout	35	Philippines	07 Apr 2001
Northeast blackout of 1965	30	United States, Canada	9 Nov 1965
2019 Venezuelan blackouts	30	Venezuela	7 Mar-26 Apr 2019
2016 Sri Lanka blackout	21	Sri Lanka	13 March 2016

Table 2.1: List of the largest power outages in history. Data from [6].

trical power systems or the smart grids, since a power system failure can have far-reaching and higher-order effects on the economy as well as most aspects of life, and also impair the operation of other critical infrastructures [39]. With the capabilities we construct that allow power to be transferred over hundreds of miles, it also enables the propagation of local failures into grid-wide events [33]. A typical example is the August 2003 blackout, where the power outage spread widely throughout parts of the Northeastern and Midwestern United States and the Canadian province of Ontario; see Figure 2.2 for the satellite photo. The outage affected an estimated 10 million people in Ontario and 45 million people in eight U.S. states. The cause of the blackout is a software bug causing operators to remain unaware of the need to redistribute load after overloaded transmission lines drooped into foliage, and what should have been a manageable local blackout cascaded into collapse of the entire North East Region [40]. At the same year, the Italy blackout affected 55 million of people, and blackouts continue to

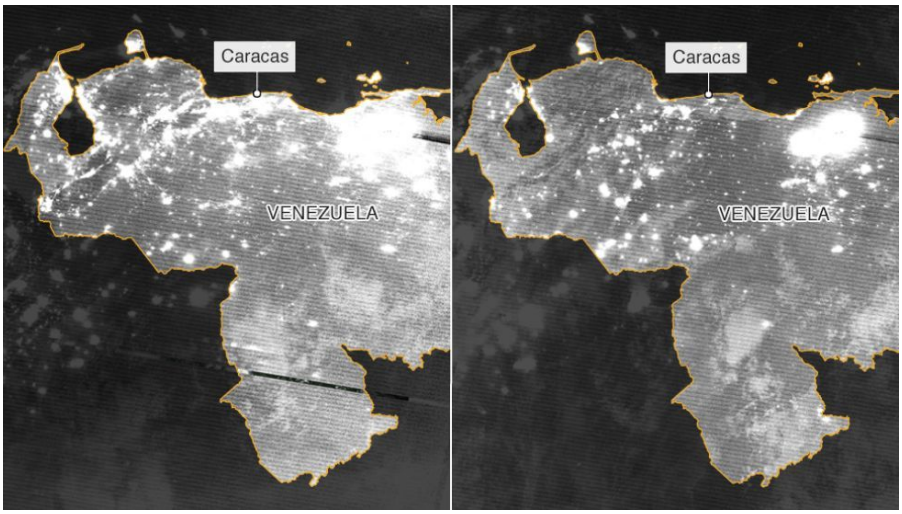


Figure 2.1: *A light map of Venezuela on the night of 7 March 2019 and the night of 8 March 2019 [1].*

happen with more and more sever impact: in the 2012 India blackouts, 620 million people was affected; the 2014 Bangladesh blackout affected 150 million people; and the 2015 Pakistan blackout caused 140 million people to lose power [6], just name a few (see table 2.1 for more information). Actually, the most recent blackout, 2019 Venezuelan blackouts, is till going [1]. The nationwide recurring electrical blackouts began in March 2019, and was the largest power outage in the country's history. It causes serious problems in hospitals and clinics, industry, transport and in water service. At least 43 deaths resulted (see Figure 2.1 for the light map of Venezuela during the blackout).

Actually, analysis of North American Electrical Reliability Council blackout data suggests the existence of blackout size distributions with power tails. Power tails decay as according to a power law and are also exhibited by complex systems near criticality. This is an indication that blackout dynamics behave as a complex dynamical system [41]. These observations indicate the non-Gaussian character of the blackout size probability distributions and are of concern because they indicate a much larger risk of large blackouts than might be expected [42], which is also shown in the recent large blackouts listed in table 2.1.

Besides power systems, cascading failures also happen in other areas of social and economical systems that greatly our daily lives. For example, in the event of a hurricane evacuations,

Figure 2.2: *A satellite photo showing the dark swath cut by the outages in the August 2003 Northeast blackout [2].*

cascading failure is a critical factor that affect transportation systems, where signal failure and subway suspension may happen that lead to the capacity loss of roadway network in evacuation [43]. Cascading failures in the Internet has also been a critical issue, in that the traffic is rerouted to bypass malfunctioning routers that eventually lead to an avalanche of overloads on other routers [44]. In wireless sensor networks(WSN), the studies are now turning away from the traditional focus on impacts of network topology and consider the impact of cascading failures brought by redistribution of network load. In this scenario, the load of a sensor node is defined as the number of data packets it's processing, and is limited by its capacity. When a node fails, the transmitted data will choose a new route to continue transmission, and network load will be redistributed. The redistribution of network load may further cause new nodes to overload and fail, thus trigger a cascade of failures. In WSNs, due to the existence of cascading failures, even though most failures emerge very locally, the entire network can be largely affected or even collapsed globally [45]. Besides the aforementioned social and technology systems, cascading failures can also happen in financial and economic networks. In light of global economic convergence, economic entities and financial markets become increasingly intertwined, and a shock in a financial network can provoke significant cascading failures throughout the global economic system [46]. Another example in economical systems is the case of firms' adaptive strategies against disruptions in a supply chain network [47]. In the disruption propagation process under this scenario, if an agent needs to find an alternative

supplier due to the failure of one of its original suppliers, this agent's operation will be disrupted if he cannot secure one such supplier. As a results, all its customers will need to seek alternative suppliers, leading to consecutive removal of nodes from the supply chain network that result the cascading failures across the whole network. The effect of cascading failures is also studied in risk and reliability assessment of complex infrastructure systems [48].

As we mentioned before, as infrastructures especially critical infrastructures such as power system, water system and traffic systems are becoming more interdependent and more interactive, a small failure can get amplified due to inherent infrastructure interdependencies and cause system-wide cascading failures. Thus, there is an increasing need to develop models and analytical tools for studying the robustness of interdependent systems when cascading failures happen. In the next section, we will introduce some existing load redistribution models in the failure process, and see their benefits and limitations.

2.2 Load redistribution models for cascading failures

The study of network failures, or resistance of networks to the removal of nodes or edges due to random breakdowns or intentional attacks, starts with the static properties of the network. This means that such studies focuses on the removal of a group of nodes and the corresponding consequences on the network performance [49–54]. Following such approach, it has been shown that the deleterious consequences happen in the network when a sizable group of nodes are removed. However in many real world systems such as the power network, the failure of a single or very small portion of the nodes can cause system-wide collapses, due to the dynamics of flow redistribution on the networks. Thus dynamic approaches have been developed to take into consideration of this phenomenon [38, 44, 55, 55–58]. In these models that involve dynamic approaches, usually each node in the network is characterized by a given initial load and capacity. Initially, the network is stable in that the load at each node is smaller than its capacity. The removal of breakdown of a node changes the balance of the flow and leads to a redistribution of loads over other nodes. If the capacity of these nodes cannot handle the extra

load, more failure will happen, and the loads from failed nodes will be redistributed again, triggering a cascade of failures that results in a large portion of malfunction or even collapse in the network.

One of the most influential model on this topic is by Motter and Lai [59], where they focus on cascades triggered by the removal of a single node. In their model, it is assumed that at each time step one unit of relevant quantity is exchanged between any pair of nodes along the shortest path, so the load at each node is defined as the number of shortest paths passing through this node. In other words, the authors used betweenness centrality to define the load. The capacity C_j of node j is defined as proportional to its initial load L_j by a tolerance parameter α; i.e., $C_j = (1+\alpha)L_j, \quad j = 1, 2, \cdots, N$. Cascading happens due to the removal of nodes since the distribution of shortest paths changes, and the load at a node can then change and may further fail due to the load being greater than the capacity. Since the load is defined as the shortest path, their results on the global cascades relies on the topology of the network involved. Their results show that when the network is highly heterogeneous and one of the the high-load nodes is removed, global cascades can occur.

Subsequent studies introduced alternative measures for the network load, such as the work of Crucitti et. al. [44] where load is defined as the number of most efficient paths passing through certain node. They also focus on cascading failures caused by removing a single node, and both random removals and load-based removals were discussed in their model. Again, since the load is defined according to the topology, they have the same results that the breakdown of a single node is sufficient to collapse a network if the node is among the ones with the largest load. There also appeared more realistic redistribution mechanisms [44, 60–62].

In the aforementioned models, the redistribution of loads is treated in a time-independent or static way, so they are also called static overload failure models. In other words, the load redistributions are instantaneously and discontinuously switched to the stationary loads of the new network, without any consideration of the transient dynamics in between. For this reason, Simonsen et. al. [63] suggested to take into account the dynamical flow properties, and

proposed a dynamical overload failure model for cascading failures. They study the transient dynamical effects as well as overload situations before the stationary state is reached, and show that the transient dynamics is often characterized by overshooting and/or oscillations in the loads, which may result in characteristic "failure waves" spreading over the network. They also show that cascading failures is generally given by a complex interplay between the network topology and flow dynamics.

2.3 Study on cascading failure of interdependent networks

Robustness of networks under the giant-component based failure model has been extensively analyzed in the case of *single* networks [5, 64, 65]. The focus has recently been shifted towards *interdependent* networks with the work of Buldyrev et al. [9], where robustness of two interdependent networks, both operating under the giant-component based intra-dependence rule, was studied. This model considers two networks of the same size, say networks A and B, where a one-to-one correspondence between nodes in each network is defined. Furthermore, it is assumed that a node in either network can function only if it's corresponding support node in the other network is functioning. To simulate the cascading failures, initially $1-p$ fraction of nodes are removed from network A along with links attached to them. Due to the dependence between networks, all nodes in network B that are connected to the removed A-nodes will also be removed, which in turn may cause further failures from A and triggering an avalanche of cascading failures. To evaluate the robustness of the interdependent networks, the size of the giant component of both networks are computed at each stage of the the failure process until a steady state is reached and no more failures happen. The authors show in their results that a broader degree distribution increases the vulnerability of interdependent networks to random failure, which is opposite to how a single network behaves.

This work has received much attention and inspired the study of interdependent networks

in many different directions. For example, in [66], the authors studied cascading failures of two coupled network with multiple connectivity links, and under the initial scenario when both networks are randomly attacked. In [11, 67], the mitigation strategy of partially decoupling the networks by creating some autonomous nodes is studied, and the problem of balancing the disconnection of interdependent links and system functionality is discussed. This strategy is shown to mitigate the system-wide failure by changing the first-order transition to a second-order, or a smooth transition, when computing the fraction of nodes in the giant component. The case of targeted attacks on high or low degree nodes is studied in [68], by using a technique that can map the targeted attack problem to the random attack problem in a transformed pair of interdependent networks. in [12], the authors studied the correspondently coupled networks, where the mutually dependent nodes have the same number of connectivity links, or the interdependent networks have identical degrees of mutually dependent nodes. In [69], the optimal strategy to allocate inter-links against random attacks are studied without specifying the topology of each individual network. The more realistic cases of interdependent systems are studied in [70, 71]. In [72], the authors consider a sandpile model on modular random graphs to study the cascade of load in an interdependent network. In this formulation, the initial load is dropped as grains uniformly distributed from zero to one less than its degree on the nodes, and the capacity of nodes are defined as their degree so that each node shed one grain (load) to each neighbor upon failure. Each network has its own distribution, with a fixed fraction of neighbors within the network and the rest connected to the other network. Using a multitype branching process, the authors show the effects of interconnections and the optimal connectivity level to balance the trade-offs.

We can see that the literature on robustness of interdependent systems focus heavily on the study of structure changes in the dynamics, especially percolation based rules where only the giant component of the graph can function, and all small components are regarded failed. Even if load is considered, the composition and redistribution of load is often closely related to the topology; for example betweenness centrality is used to define the load in many cases, which

itself is a measure for network structure. In many real world systems, the load is a specific physical commodity, such as electricity or water, instead of abstract of topology features. And the redistribution of load is often times not only restricted by topology; for example long term effect in the power system is observed where the failure of nodes not only affect neighboring areas but has influenced the load in regions far away. On the other hand, very few studies consider engineering aspects of inter-dependent networks and very little is known as to how such systems can be designed to have maximum robustness under certain design constraints; see [22–25] for rare exceptions. The current literature is also lacking interdependent system models that enable studying robustness of systems that integrate networks with inherently different behavior. For example, in cyber-physical systems, it would be expected that the functionality of the physical subsystem is primarily governed by the physical flows and capacities associated with its components, whereas system-wide connectivity would be the prominent requirement for maintaining functionality in the cyber network. There is thus a need to develop new approaches for modeling and analyzing cascading failures in interdependent networks. In the following chapters of this thesis, we will introduce our models that takes into consideration the aforementioned factors, and provide detailed analytic results in the case of a flow-redistribution network and an interdependent network.

Part II

Robustness of Flow-carrying Networks

Chapter 3

Flow-carrying Networks under Random Attacks

In this chapter, we build a simple yet useful model to study the robustness of flow-carrying networks against cascading failures. We will focus on cascading failures caused by random attacks in this chapter, and the case of targeted attack will be discussed in the next chapter. We will introduce motivation, the formulation of the model, give a comprehensive analytical results including the proof of the optimal robustness, then verify our analysis with various simulation results from both synthetic data and real-world data.

3.1 Motivation and problem statement

Our study of flow-carrying networks is motivated by the concern of vulnerabilities of flow-carrying networks such as power networks, traffic networks, etc. Flow-carrying networks are often among the most critical national infrastructures that affect all areas of daily life, for example electrical power systems provide crucial support for other national infrastructures such as telecommunications, transportation, water supply systems and emergency services. However, several large-scale failures happened recently around the world rises the concern for these critical flow-carrying infrastructures. For example, in the 2012 India blackout, 600 million people, nearly a tenth of the world's population, were left without power [73, 74].

These large-scale failures often start with natural hazards such as lightning shorting a line or with malicious attacks, and affect only a small portion of the network initially. But due to the nature of the physical commodity carried, such as the long range nature of electricity,

the redistribution of loads (or flow) may affect not only geographically co-located nodes or lines but also other parts of the system far from the initial affected area, as history records show [75]. The large-scale blackouts in power systems are often attributed to this initial shock getting escalated due to the intricate dependencies within a power system. For example, when a line is tripped, the flow on all other lines will be updated, and some lines may end up with a total flow (initial plus redistributed after failures) exceeding their capacity. All lines with flows exceeding their capacity will in turn fail and flows on other lines will be updated again, possibly leading to further failures, and so on. This process may continue recursively and lead to a cascade of failures, which may potentially breakdown the entire system.

Since these critical infrastructures such as electrical power systems are among the largest and most complex technological systems ever developed [76], it is often hard to have a full understanding of their inter- and intra-dependencies and therefore it is hard to predict their behavior under external attacks or random failures. In this work, we aim to shed light on the robustness of such flow-carrying networks using a simple yet useful model. In particular, we assume that when a line fails, its load (i.e., flow) is redistributed *equally* among all other lines. The equal load redistribution model has the ability to capture some critical character of the network, such as the *long-range* nature of the Kirchhoff's law, at least in the mean-field sense, as opposed to the *topological* models where failed load is redistributed only *locally* among neighboring lines [77, 78]. This is particularly why this model received recent attention in the context of power systems first in the work by Pahwa et al. [79] and then in Yağan [80]; the model is originally inspired by the *democratic fiber-bundle model* [81] that is used extensively for studying the rupture of fiber-bundles under increasing external force.

Our main goal is to study the robustness of flow-carrying networks under the equal load-redistribution model. In this work, we assume that failures are initiated by a *random* attack (or failure) that results with a failure of $1-p$ fraction of the lines. In other words, only p fraction of lines are alive after the initial failure. The initial failures lead to redistribution of flows from the failed lines to *alive* ones (i.e., non-failed lines), so that the load on each alive line becomes

its initial load plus its equal share of the total load of the failed lines. This may lead to the failure of some additional lines due to the updated flow exceeding their capacity. This process may continue recursively, generating a *cascade of failures*, with each failure further increasing the load on the alive lines, and may eventually result with the collapse of the entire system. Throughout, we let $n_\infty(p)$ denote the expected *final* fraction of alive lines when $1-p$ fraction of lines is randomly attacked:

$$n_\infty(p) := \lim_{N\to\infty} \frac{\mathbb{E}\left[|\mathcal{N}_{\text{surviving}}(p)|\right]}{N} \tag{3.1}$$

where $\mathcal{N}_{\text{surviving}} \subset \{1,\ldots,N\}$ is the set of lines that are still functioning at the steady state. The *robustness* of a flow-carrying network will be evaluated by the behavior $n_\infty(p)$ for all attack sizes with $0 < p < 1$. Of particular interest is to characterize the *critical* attack size $1-p^\star$ at which $n_\infty(p)$ drops to zero.

We believe that our results provide interesting insights into the dynamics of cascading failures in such systems. In particular, we expect our work to shed some light on the *qualitative* behavior of real-world systems under random attacks, and help design them in a more robust manner. Although we set the example mainly in power systems, the results obtained here may have applications in other fields as well. A particularly interesting application is the study of the traffic jams in roads, where the capacity of a line can be regarded as the traffic flow capacity of a road [82, 83].

3.2 Model definition

Equal load-redistribution model. We consider a flow-carrying system, such as a power system, with N transmission lines $\mathcal{L}_1,\ldots,\mathcal{L}_N$ with initial loads (i.e., power flows) $L_1,\ldots,L_N$. The *capacity* C_i of a line $\mathcal{L}_i$ defines the maximum flow that it can sustain, and is given by

$$C_i = L_i + S_i, \qquad i = 1,\ldots,N, \tag{3.2}$$

where S_i denotes the *free-space* (or, redundancy) available to line $\mathcal{L}_i$. The capacity of a line can be defined as a factor of its initial load, i.e.,

$$C_i = (1 + \alpha_i)L_i \tag{3.3}$$

with $\alpha_i > 0$ defining the *tolerance* parameter for line $\mathcal{L}_i$. Put differently, the free space S_i is given in terms of the initial load L_i as $S_i = \alpha_i L_i$; it is very common [59,77,84,85] to use a *fixed* tolerance factor for all lines in the system, i.e., to use $\alpha_i = \alpha$ for all i. It is assumed that a line *fails* (i.e., outages) if its load exceeds its capacity at any given time. The key assumption of our model is that when a line fails, the load it was carrying (right before the failure) is redistributed *equally* among all remaining lines.

Throughout we assume that the pairs (L_i, S_i) are independently and identically distributed with $P_{LS}(x, y) := \mathbb{P}[L \leq x, S \leq y]$ for each $i = 1, \ldots, N$. The corresponding (joint) probability density function is given by $p_{LS}(x, y) = \frac{\partial^2}{\partial x \partial y} P_{LS}(x, y)$. Throughout, we let L_{min} and S_{min} denote the minimum values for load L and free space S; i.e.,

$$L_{min} = \inf\{x : P_L(x) > 0\}$$
$$S_{min} = \inf\{y : P_S(y) > 0\}$$

We assume that $L_{min}, S_{min} > 0$. We also assume that the marginal densities $p_L(x)$ and $p_S(y)$ are continuous on their support.

3.3 Main results

3.3.1 Final system size

Our first main result characterizes the robustness of the network under any initial load-space distribution P_{LS} and any attack size $1-p$. Let L and S denote generic random variables follow-

ing the same distribution with initial loads $L_1, \ldots, L_N$, and free spaces $S_1, \ldots, S_N$, respectively. Then, with $x^\star$ denoting the smallest solution of

$$h(x) := \mathbb{P}\left[S > x\right]\left(x + \mathbb{E}\left[L \mid S > x\right]\right) \geq \frac{\mathbb{E}\left[L\right]}{p} \tag{3.4}$$

over the range $x^\star \in (0, \infty)$, the expected final system size $n_\infty(p)$ at attack size $1 - p$ is given by

$$n_\infty(p) = p\mathbb{P}\left[S > x^\star\right]. \tag{3.5}$$

This result provides a complete picture about a flow-carrying network's robustness against random attacks of arbitrary size. In particular, it helps understand the response $n_\infty(p)$ of the system to attacks of varying magnitude.

Figure 3.1 shows the analytic results and simulation results of final system size. We see from this result that an adversarial attack aimed at a certain part of the electrical power grid may lead to failures in other parts of the system, possibly creating a recursive failure process also known as *cascading failures*. This will often result with a damage in the system much larger than the initial attack size $1 - p$. However, in most cases "some" part of the system is expected to continue its functions by undertaking extra load; e.g., with $n_\infty(p) > 0$. In such cases, although certain service areas are affected, the system such as power grid remains partially functional. The most severe situations arise when cascading failures continue until the *complete* breakdown of the system where all lines fail; e.g., when $n_\infty(p) = 0$. This prompts us to characterize the *critical* attack size $1 - p^\star$, defined as the largest attack size that the system can sustain.

3.3.2 The critical attack size

Of particular interest is to derive the *critical* attack size $1-p^\star$ such that for any attack with size $1 - p > 1 - p^\star$, or the initially survived line fraction $p < p^\star$,the system undergoes a complete breakdown leading to $n_\infty(p) = 0$; on the other hand for $p > p^\star$, we have $n_\infty(p) > 0$. More

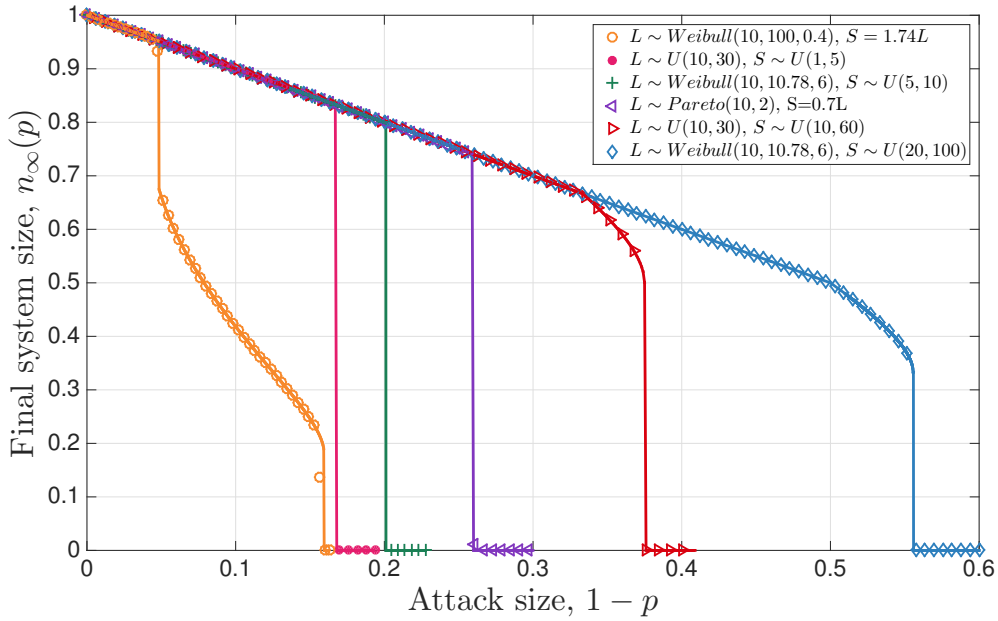


Figure 3.1: *Final system size under different load-free space distributions. Analytic results (obtained from (3.4) and (3.5)) are represented by lines, whereas simulation results (averaged over 200 independent runs) are represented by symbols. We see that in each case theoretical results match the simulation results very well.*

precisely, we define $1 - p^\star$ as

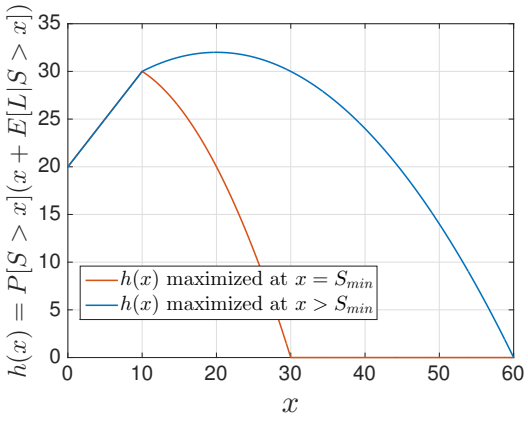
$$1 - p^\star = \inf\{p : n_\infty(p) > 0\}.$$

The critical attack size can be derived from the previous results (3.4)-(3.5) that characterize $n_\infty(p)$.Namely, for any load-free space distribution $p_{LS}(x, y)$, the maximum attack size $1 - p^\star$ can be computed from the *global* maximum of the function $\mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])$. In particular, we have

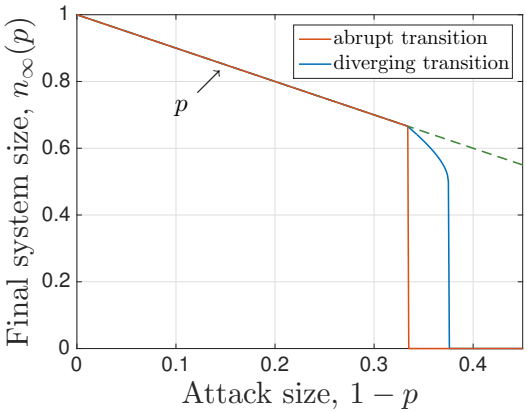
$$1 - p^\star = \frac{\mathbb{E}[L]}{\max\limits_x \{\mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])\}}. \tag{3.6}$$

3.3.3 Phase transitions and abrupt rupture

It is of significant interest to understand the behavior of the system near the *phase transition*; i.e., when the attack size is very close to but smaller than the critical value $1 - p^\star$. One



(a)



(b)

Figure 3.2: *Different types of first-order transitions. We demonstrate the difference between an* abrupt *first-order transition and a first-order transition with a preceding divergence from the p line. The lower curves (shown in red) correspond to the case where the load L and extra space S are independent and uniformly distributed with $L_{min} = S_{min} = 10$ and $\mathbb{E}[L] = \mathbb{E}[S] = 20$. The upper curves (shown in blue) are obtained under the same setting except that we set $\mathbb{E}[S] = 35$. We see that the lower curve in Figure 3.2a reaches its maximum at $S_{min} = 10$, and the corresponding final system size exhibits an* abrupt *first-order transition as shown in Figure 3.2b. On the other hand, the upper (i.e., blue) curve in Figure 3.2a is maximized at $S = 20 > S_{min}$. As expected from our result (e.g., see (3.8)), the total breakdown of the system takes place after a diverging failure rate is observed.*

main questions here is whether $n_\infty(p)$ decays to zero continuously (i.e., through a second-order transition), or discontinuously (i.e., through a first-order transition). The practical significance of this is that continuous transitions suggest a more stable and predictable system behavior with respect to attacks, whereas with discontinuous transitions system behavior becomes more difficult to predict, for instance, from past data. Our analysis shows that under the equal-load redistribution model considered here the total breakdown of the system will always be through a first-order (i.e., discontinuous) transition. This means that regardless of the attack size and the distribution of load and capacity, the transition point where the system has a total breakdown (i.e., where the fraction of alive lines drops to zero) is always discontinuous. These cases are reminiscent of the real-world phenomena of unexpected large-scale system collapses; i.e., cases where seemingly identical attacks/failures leading to entirely different consequences.

Now that we showed that the breakdown of the power system takes place through a first-

order transition, an interesting question arises as to whether this first-order rupture at $1-p^\star$ has any early indicators at smaller attack sizes; e.g., a *diverging* failure rate leading to a non-linear decrease in $n_\infty(p)$. Otherwise, an *abrupt* first-order transition is said to take place if the linear decay of $n_\infty(p)$ is followed by a sudden discontinuous jump to zero at $1-p^\star$; i.e., we say that the system exhibits an *abrupt* rupture when it holds that

$$n_\infty(p) = \begin{cases} p & \text{if } 1-p \leq 1-p^\star \text{ or } p > p^\star \\ 0 & \text{if } 1-p > 1-p^\star \text{ or } p < p^\star \end{cases} \tag{3.7}$$

In Figure 3.2b we demonstrate the distinction between an *abrupt* rupture and a rupture with preceding divergence from the p line.

We show that the system goes through an abrupt first-order breakdown (e.g., see the below line shown in red in Figure 3.2b), if and only if the function $h(x) = \mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])$ reaches its maximum at $x = S_{min}$, where S_{min} is the minimum value the extra space S can take. Namely, an abrupt first-order rupture (*without* a preceding divergence) takes place if and only if

$$\arg\max_{x>0} \{\mathbb{P}\left[S > x\right](x + \mathbb{E}\left[L \mid S > x\right])\} = S_{\min}. \tag{3.8}$$

Otherwise, if $\arg\max_{x>0} h(x) \neq S_{\min}$, then a preceding divergence from the p line will be observed before $n_\infty(p)$ drops to zero; e.g., see the above line shown in blue in Figure 3.2b). More precisely, it will hold that $n_\infty(p) < p$ for some $p > p^\star$.

3.3.4 Achieving optimal robustness

The most important question from a system design perspective is concerned with deriving the *universally optimum* distribution of initial loads $L_1, \ldots L_N$ and free spaces $S_1, \ldots, S_N$ that leads to *maximum* robustness under the constraints that $\mathbb{E}\left[L\right]$ and $\mathbb{E}\left[S\right]$ are fixed. We believe that the answer to this problem would be very useful in designing real-world power grids with optimum robustness, i.e. with the final system size $n_\infty(p)$ maximized for any attack size p.

The motivation for the constraints on the mean load $\mathbb{E}[L]$ and mean free space $\mathbb{E}[S]$ are as follows. The total load carried by the system is likely to be dictated by system requirements in most real-world cases, which also determines the average load per line. In addition, the total capacity (or, total free space) available to the system is likely to be bounded due to the *costs* associated with using high-capacity lines.

Our results concerning this important problem are presented next. First, we focus on maximizing the critical attack size $1 - p^\star$. We show in Methods that the critical attack size always satisfies

$$1 - p^\star \leq \frac{\mathbb{E}[S]}{\mathbb{E}[S] + \mathbb{E}[L]} = \frac{\mathbb{E}[S]}{\mathbb{E}[C]} \tag{3.9}$$

Namely, regardless of the distribution p_{LS} that generates load-capacity pairs, the system will always go into a complete breakdown if more than $\mathbb{E}[S]/\mathbb{E}[C]$-fraction of lines are attacked; i.e., the system can never sustain a random attack of size exceeding the ratio of mean free space to mean capacity. Next, we show that this critical attack size is in fact attainable *under any load distribution* by a *Dirac* delta distribution for the free-spaces, i.e., by giving every line the same free space. More precisely, let $p^\star_{dirac}$ denote the critical attack size when $p_{LS}(x, y) = p_L(x)\delta(y - \mathbb{E}[S])$, where the distribution $p_L(x)$ of the initial loads $L_1, \ldots, L_N$ is arbitrary. We show in Methods that

$$1 - p^\star_{dirac} \geq \frac{\mathbb{E}[S]}{\mathbb{E}[S] + \mathbb{E}[L]}.$$

Combined with (3.9) this shows that assigning every line the same free space (regardless of the initial loads) maximizes the largest attack that the system can sustain.

More can be said regarding the optimality of equal free-space allocation. Let $1 - p^\star_{optimal}$ denote the maximum critical attack size as established above, i.e., $1 - p^\star_{optimal} = \mathbb{E}[S]/(\mathbb{E}[S] + \mathbb{E}[L])$. In view of the fact that we always have $n_\infty(p) \leq p$, the next result firmly establishes that using the Dirac delta distribution for free space optimizes the robustness of the system uniformly for any attack size p. In particular, if $p_{LS}(x, y) = p_L(x)\delta(y - \mathbb{E}[S])$, then the

corresponding final system size $n_{\infty,dirac}(p)$ satisfies

$$n_{\infty,dirac}(p) = \begin{cases} p & \text{for } 1-p < 1-p^{\star}_{optimal} \\ 0 & \text{for } 1-p \geq 1-p^{\star}_{optimal} \end{cases} \tag{3.10}$$

Namely, the distribution $p_{LS}(x,y) = p_L(x)\delta(y - \mathbb{E}[S])$ maximizes the final system size $n_\infty(p)$ uniformly for all p.

This result shows that as far as the *random* attacks are concerned, the system's robustness can be maximized under the constraints of fixed $\mathbb{E}[L]$ and fixed $\mathbb{E}[S]$ (and hence fixed $\mathbb{E}[C]$), by giving each line an equal free space $\mathbb{E}[S]$, **irrespective of how the initial loads are distributed**. Put differently, the robustness will be maximized by choosing a line's capacity C_i through $C_i = L_i + \mathbb{E}[S]$ no matter what its load L_i is.

A possible explanation to this result is as follows. When all lines have the same extra space, we ensure that the system never goes through a *cascade* of failures. In other words, when $1-p$ fraction of the lines are attacked, we will have either $n_\infty(p) = p$ or $n_\infty(p) = 0$ depending on whether or not, respectively, the total load of failed lines divided by p is less than the common free space S. In addition, if the attack size is large enough that total load of failed lines, i.e., $(1-p)\mathbb{E}[L]$, is larger than the total free space $p\mathbb{E}[S]$ available in the rest of the system, then regardless of the distribution $p_{LS}(x,y)$, the system will collapse. Collectively, these explain why assigning equal free-space to all lines ensures that system will go through an abrupt rupture, but only at the optimal critical attack size $p^{\star}_{optimal}$.

3.4 Simulation results

We now confirm our theoretical findings via numerical simulations, using both synthetic and real-world data. We focus on the former case first and consider various commonly known distributions for the load and free-space variables.

Synthetic data. Throughout, we consider three commonly used families of distributions:

i) Uniform, ii) Pareto, and iii) Weibull. The corresponding probability density functions are defined below for a generic random variable L.

- Uniform Distribution: $L \sim U(L_{\min}, L_{\max})$. The density is given by

$$p_L(x) = \frac{1}{L_{\max} - L_{\min}} \cdot \mathbf{1}\left[L_{\min} \leq x \leq L_{\max}\right]$$

- Pareto Distribution: $L \sim Pareto(L_{\min}, b)$. With $L_{\min} > 0$ and $b > 0$, the density is given by

$$p_L(x) = L_{\min}^b b x^{-b-1} \mathbf{1}\left[x \geq L_{\min}\right].$$

  To ensure that $\mathbb{E}[L] = bL_{\min}/(b-1)$ is finite, we also enforce $b > 1$. Distributions belonging to the Pareto family are also known as a *power-law* distributions and have been extensively used in many fields including power systems.

- Weibull Distribution: $L \sim Weibull(L_{\min}, \lambda, k_w)$. With $\lambda, k_w, L_{\min} > 0$, the density is given by

$$p_L(x) = \frac{k_w}{\lambda}\left(\frac{x - L_{\min}}{\lambda}\right)^{k_w - 1} e^{-\left(\frac{x - L_{\min}}{\lambda}\right)^{k_w}} \mathbf{1}\left[x \geq L_{\min}\right].$$

  The case $k_w = 1$ corresponds to the exponential distribution, and $k_w = 2$ corresponds to Rayleigh distribution. The mean load is given by $\mathbb{E}[L] = L_{\min} + \lambda\Gamma(1 + 1/k_w)$, where $\Gamma(\cdot)$ is the gamma-function given by $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$.

First, we confirm our results presented in Sections 3.3.1 and 3.3.3 concerning the response of the system to attacks of varying size; i.e. concerning the final system size $n_\infty(p)$ under different load-extra space distributions including its transition behavior around the critical attack size $1 - p^\star$. In all simulations, we fix the number of lines at $N = 10^6$, and for each set of parameters being considered (e.g., the distribution $p_{LS}(x, y)$ and attack size p) we run 200 independent experiments. The results are shown in Figure 3.1 where symbols represent the *empirical* value of the final system size $n_\infty(p)$ (obtained by averaging over 200 independent runs for each data

point), and lines represent the analytical results computed from (3.4) and (3.5). We see that theoretical results match the simulations very well in all cases.

The specific distributions used in Figure 3.1 are as follows: From left to right, we have i) L is Weibull with $L_{\min} = 10, \lambda = 100, k_w = 0.4$ and $S = \alpha L$ with $\alpha = 1.74$; ii) L is Uniform over [10,30] and S is Uniform over [1,5]; iii) L is Weibull with $L_{\min} = 10, \lambda = 10.78, k_w = 6$ and S is Uniform over [5,10]; iv) L is Pareto with $L_{\min} = 10, b = 2$, and $S = \alpha L$ with $\alpha = 0.7$; v) L is Uniform over [10,30] and S is Uniform over [10,60]; and vi) L is Weibull with $L_{\min} = 10, \lambda = 10.78, k_w = 6$ and S is Uniform over [20,100]. Thus, the plots in Figure 3.1 demonstrate the effect of the load-free space distribution on the robustness of the resulting power system. We see that both the *family* that the distribution belongs to (e.g., Uniform, Weibull, or Pareto) as well as the specific parameters of the family affect the behavior of $n_\infty(p)$. For instance, the curves representing the two cases where L and S follow a Uniform distribution demonstrate that both *abrupt* ruptures and ruptures with a preceding divergence are possible in this setting, depending on the parameters $L_{\min}, L_{\max}, S_{\min}$ and $S_{\max}$. In cases where the load follows a Pareto distribution and $S = \alpha L$, only abrupt ruptures are possible as shown in [80]. Finally, we see that the Weibull distribution gives rise to a richer set of possibilities for the transition of $n_\infty(p)$. Namely, we see that not only we can observe an abrupt rupture, or a rupture with preceding divergence (i.e., a second-order transition followed by a first-order breakdown), it is also possible that $n_\infty(p)$ goes through a first-order transition (that does not breakdown the system) followed by a second-order transition that is followed by an ultimate first-order breakdown; see the behavior of the orange circled line in Figure 3.1. We remark that these cases occur when $h(x)$ has a local maximum at $x = S_{min}$, while its global maximum occurs at a later point $x > S_{min}$; see [80] for a more detailed discussion of this matter.

In our second set of simulations we seek to verify the results presented in Section 3.3.4, namely the optimality of assigning the same free space to all lines (regardless of how initial loads are distributed) in terms of maximizing the robustness. In the process, we also seek to compare the robustness achieved under equal free-space distribution versus the commonly used

strategy of setting $S_i = \alpha L_i$ for each line. We note that the latter setting with a universal tolerance factor α is commonly used in relevant research literature [59, 77, 84, 85] as well as in industrial applications [38, 86]; therein, the term $(1+\alpha)$ is sometimes referred to as the *Factor of Safety*. The results are depicted in Figure 3.4 where lines represent the analytical results given in Section 3.3.4 and symbols are obtained by averaging over 200 independent experiments with $N = 10^6$ lines. In all cases we fix the mean load at $\mathbb{E}[L] = 30$ and mean free-space at $\mathbb{E}[S] = 10$. With load distributed as Uniform (Figure 3.4a), Weibull (Figure 3.4b), or Pareto (Figure 3.4c), we either let $S_i = 10$ for all lines, or use $S_i = \alpha L_i$ with $\alpha = \mathbb{E}[S]/\mathbb{E}[L] = 1/3$, the latter choice making sure that the mean free-space is the same in all plots.

We see in all cases that there is an almost perfect agreement between theory and simulations. We also confirm that regardless of how initial load is distributed, the system achieves uniformly optimal robustness (i.e., maximum $n_\infty(p)$ for all p) as long as the free-space is distributed equally; e.g., see Figure 3.4d that combines all plots in Figures 3.4a-3.4c. In other words, we confirm that (3.10) holds with the critical attack size $1 - p^\star$ matching the optimal value $1 - p^\star_{optimal} = \mathbb{E}[S]/\mathbb{E}[C] = 0.25$. Finally, by comparing the robustness curves under equal free-space and equal tolerance factor, we see the dramatic impact of free-space distribution on the robustness achieved. To give an example, we see from Figure 3.4d that regardless of how initial load is distributed, the system can be made robust against random attacks that fail up to 25% of the lines; as already discussed this is achieved by distributing the total free-space equally among all lines. However, if the standard approach of setting the free-space proportional to the initial load is followed, the system robustness can be considerably worse with attacks targeting as low as 10% of the lines being able to breakdown the system.

Real wold data. Thus far, our analytical results are tested only on synthetic data; i.e., simulations are run when load-free space variables $\{L_i, S_i\}_{i=1}^N$ are generated *randomly* from commonly known distributions. To get a better idea of the real-world implications of our work, we also run simulations on power flow data from the IEEE power system test cases [3]; the IEEE test-cases are widely regarded as realistic test-beds and used commonly in the literature.

Here, we consider four power flow test cases corresponding to the 30-bus, 57-bus, 118-bus, and 300-bus systems. For each test case, we take the load values directly from the data-set [3]. Since the data-set does not contain the line capacities, we allocate all lines an equal free-space, $S = 10$; clearly, most of the discussion here would follow with different free-space distributions.

Figure 3.5 presents the results from the IEEE data set simulations, where blue circles represent the final system size $n_\infty(p)$ under original load data from each test case; each data point is obtained by averaging the result of 200 independent random attack experiments. As we compare these circles with our analytical results (represented by solid red lines) we see that the overall tendency of $n_\infty(p)$ is in accords with the theoretical analysis. However, the agreement of theory and simulations is significantly worse than that observed in Figures 3.1 and 3.4. This is because our mean field analysis relies on the number of lines N being *large*, while the IEEE test case data represent very small systems; e.g., the underlying systems have 30, 57, 118, and 300 lines in Figures 3.5a-3.5d, respectively. In order to verify that the mismatch is due to the small system size (rather than the load distribution being different from commonly known ones), we re-sample 10^5 load values from the *empirical* load distribution obtained from the data-set in each case; the Inset in each figure shows the corresponding empirical distribution $P_L(x)$. The simulation results with these $N = 10^5$ load values are shown in Figure 3.5 with red triangles. This time with the number of lines increased, we obtain a perfect match between analysis and simulations. This confirms our analysis under realistic load distributions as well. We also see that although analytical results fail to match the system robustness perfectly when N is very small, they still capture the overall tendency of the robustness curves pretty well. In fact, they can be useful in predicting attack sizes that will lead to a *significant* damage to the system; e.g., in all cases we see that the analytically predicted critical attack size $p^\star$, ranging from 0.42 in Figure 3.5a to 0.07 in Figure 3.5d, leads to the failure of more than 50 % of all lines in the real system.

3.5 Chapter summary

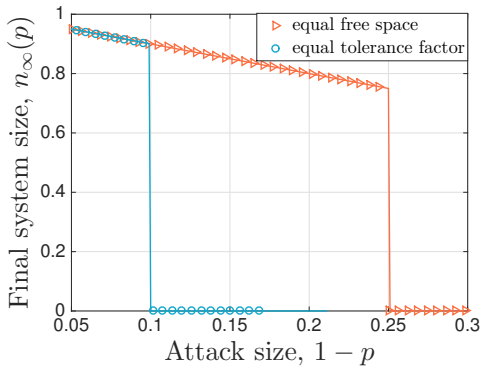
In this chapter, we introduced the equal and global redistribution model for studying robustness of flow-carrying networks against cascading failures initiated by a random attack. Our results provide a complete picture of the robustness of such systems: the analysis explains how the final system size $n_\infty(p)$ will behave under attacks with varying size $1-p$. We also demonstrate different types behavior that $n_\infty(p)$ can exhibit near and around the *critical* attack size $1-p^\star$, i.e., the point after which $n_\infty(p)=0$ and the system breaks down completely. We show that the final breakdown of the system is always first-order (i.e., discontinuous) but depending on $p_{LS}(x,y)$, this may i) take place abruptly meaning that $n_\infty(p)$ follows the p line until its sudden jump to zero; or ii) be preceded by a second-order (i.e., continuous) divergence from the p line. We also demonstrate the possibility of richer behavior where $n_\infty(p)$ drops to zero through a first-order, second-order, and then a first-order transition. The discontinuity of the final system size at $1-p^\star$ makes it very difficult to predict system behavior (in response to attacks) from previous data. In fact, this is reminiscent of the real-world phenomena of unexpected large-scale system collapses; i.e., cases where seemingly identical attacks/failures lead to entirely different consequences. On the other hand, the cases that exhibit a preceding second-order transition are less severe, since the deviation from the p line may be taken as an early warning that the current attack size is close to $1-p^\star$ and that the system is not likely to sustain attacks much larger than this.

From a design perspective, it is desirable to maximize the robustness of such system under certain constraints. In our analysis, we address this problem and derive the optimal load-free space distribution $p_{LS}(x,y)$ that maximizes the final system size $n_\infty(p)$ uniformly for all attack sizes $1-p$. Namely, we show that under the constraints that $\mathbb{E}[L]$ and $\mathbb{E}[S]$ are fixed, robustness is maximized by allocating the the same free space to all lines and distributing the initial loads arbitrarily; i.e. the distribution $p_{LS}(x,y)=p_L(x)\delta(y-\mathbb{E}[S])$ maximizes robustness for arbitrary $p_L(x)$. We show that this optimal distribution leads to significantly

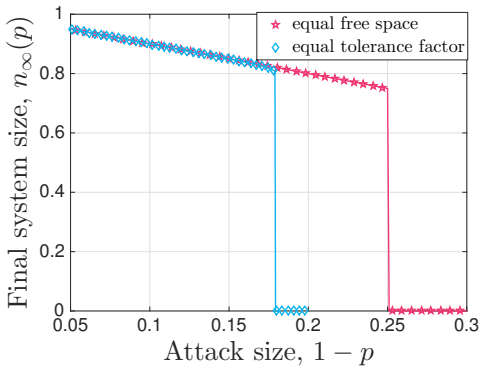
better robustness than the commonly used strategy of assigning a universal tolerance factor α, i.e., using $p_{LS}(x, y) = p_L(x)\delta(y - \alpha x)$.

Our theoretical results are verified via extensive simulations using both synthetic data and real world data. We show that our results are in perfect agreement with numerical simulations when the system size N is large; in most cases it suffices to have $N = 10^4$ to $N = 10^5$. However, we see from our simulations with the IEEE test-cases that when N is very small (we considered $N = 30$, $N = 57$, $N = 118$, and $N = 300$), our theory fails to yield the same prediction accuracy. Nevertheless, we see that our results capture the overall tendency of $n_\infty(p)$ pretty well, and thus can serve as a useful predictor of the critical attack size.

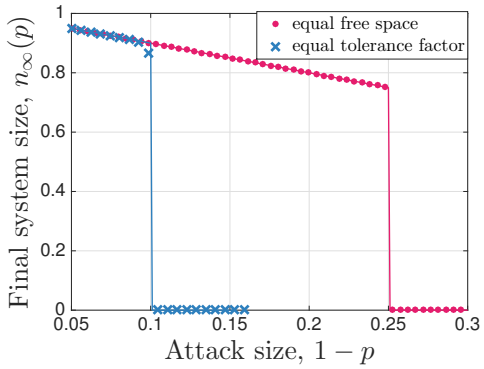
In the next chapter, we will consider the case of *targeted* attacks. We will study possible attack strategies that a capable adversary might use; e.g., given $L_1, \ldots, L_N$ and $S_1, \ldots, S_N$, which k lines should an adversary attack in order to minimize the final system size n_∞? We already know from some preliminary analysis [87] that the optimal attack strategies is NP-Hard, in other words, it is computationally expensive to derive. We will discuss this problem, as well as a modified optimization problem where the adversary is further constrained with the total load of the lines attacked, and give heuristic algorithms for both optimization problems.



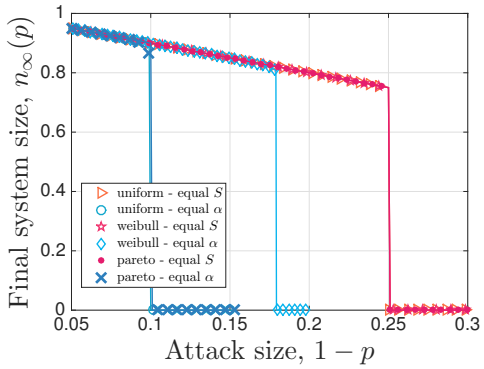
(a) Load follows Uniform distribution



(b) Load follows Weibull distribution

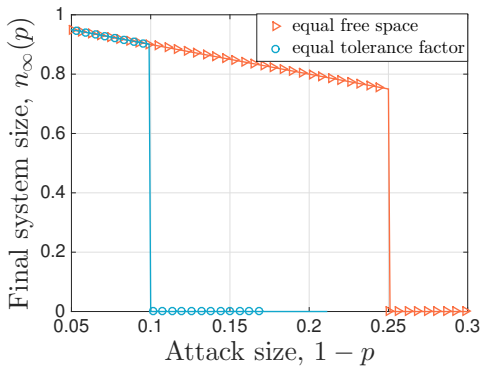


(c) Load follows Pareto distribution

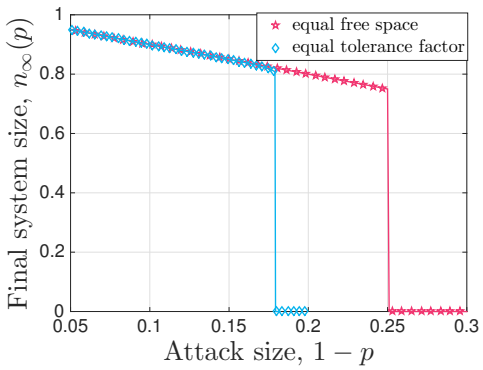


(d) Comparison of different load distribution

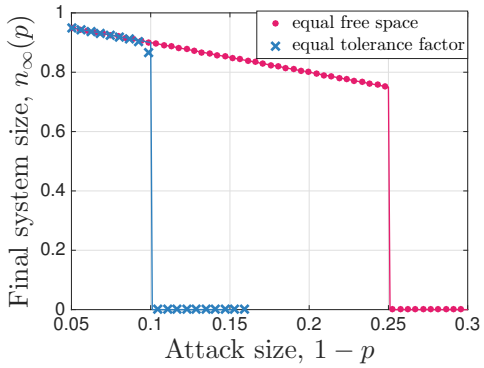
Figure 3.3: *Final system size under equal free space vs. equal tolerance factor. In all cases, we set* $L_{min} = 10$, $\mathbb{E}[L] = 30$, *and* $\mathbb{E}[S] = 10$. *When load follows Weibull distribution we let* $k_w = 6$ *and set* $\lambda = 20/\Gamma(1 + 1/k_w)$ *so that* $\mathbb{E}[L] = 30$. *In each of the three cases, we either let* $S \sim \delta(\mathbb{E}[S])$ *meaning that all lines have the same free space, or we set* $S_i = \alpha L_i$ *with* $\alpha = \mathbb{E}[L]/\mathbb{E}[S] = 1/3$ *so that the mean free space still equals 10. We see that analysis (represented by lines) match the simulations (shown in symbols) very well and that robustness is indeed optimized by equal free-space allocation regardless of how initial load is distributed. We also see that system is significantly more robust under equal free space allocation as compared to the case of the equal tolerance factor.*



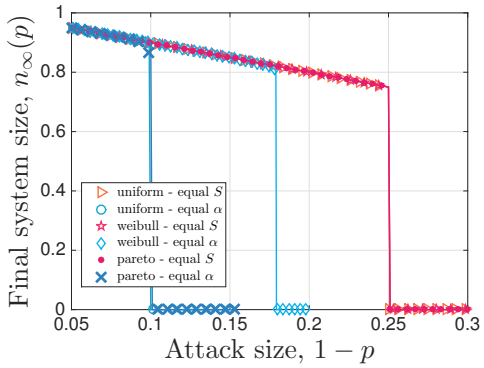
(a) Load follows Uniform distribution



(b) Load follows Weibull distribution

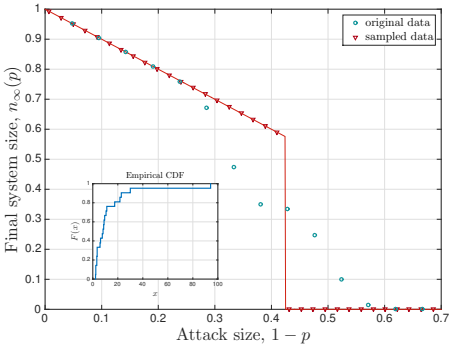


(c) Load follows Pareto distribution

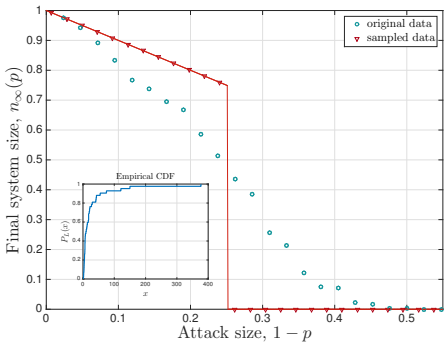


(d) Comparison of different load distribution

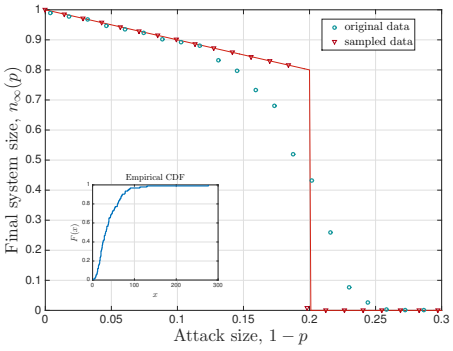
Figure 3.4: *Final system size under equal free space vs. equal tolerance factor. In all cases, we set* $L_{min} = 10$, $\mathbb{E}[L] = 30$, *and* $\mathbb{E}[S] = 10$. *When load follows Weibull distribution we let* $k_w = 6$ *and set* $\lambda = 20/\Gamma(1 + 1/k_w)$ *so that* $\mathbb{E}[L] = 30$. *In each of the three cases, we either let* $S \sim \delta(\mathbb{E}[S])$ *meaning that all lines have the same free space, or we set* $S_i = \alpha L_i$ *with* $\alpha = \mathbb{E}[L]/\mathbb{E}[S] = 1/3$ *so that the mean free space still equals 10. We see that analysis (represented by lines) match the simulations (shown in symbols) very well and that robustness is indeed optimized by equal free-space allocation regardless of how initial load is distributed. We also see that system is significantly more robust under equal free space allocation as compared to the case of the equal tolerance factor.*



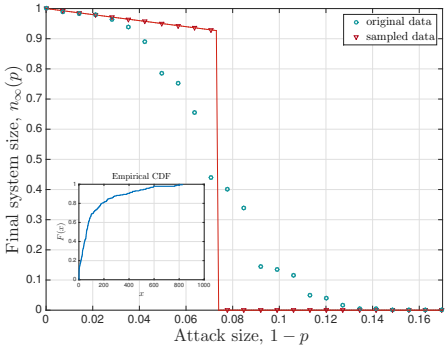
(a) IEEE 30 bus test case



(b) IEEE 57 bus test case



(c) IEEE 118 bus test case



(d) IEEE 300 bus test case

Figure 3.5: *Simulation results on IEEE test cases. The initial load values are taken directly from the corresponding IEEE test-case data-sheet [3], and each line is given an equal free space of* $\mathbb{E}[S] = 10$. *The empirical distribution of load is shown in the Inset of each figure, and the mean load values are given by 13.54, 29.95, 39.95, and 125.02 for the 30-bus system, 57-bus system, 118-bus system, and 300-bus system, respectively. The blue circles represent the simulation results for the final system size* $n_\infty(p)$. *The theoretical results (shown in lines) capture the overall tendency of* $n_\infty(p)$ *but fail to predict the numerical results well, especially around the critical attack size. We see that this is merely a finite-size effect as we sample* $N = 10^5$ *load values from the empirical distribution and repeat the same experiment. The results are shown in red triangles and are in perfect agreement with the analysis.*

Chapter 4

Flow-carrying Networks Under Targeted Attacks

4.1 Motivation and problem statement

Networks that carry or transport physical commodities, e.g., electricity, water, gas distribution networks or road, public transportation networks, have been an integral part of our daily lives for decades. We already introduced in the last section that these systems can be modeled as flow-carrying networks under a simple yet useful model, equal load-redistribution model. Namely, we consider a system, such as power grid, with N lines with initial loads $L_1, \ldots, L_N$ and capacities $C_1, \ldots, C_N$. If a line fails (for any reason), its load is assumed to be redistributed equally among all lines that are *alive*. Thus, the load carried by a line i may exceed its initial value L_i over time due to load redistribution. The capacity C_i defines the maximum flow allowed on the line i, meaning that if the load carried by i exceeds this capacity at any time, the line will be tripped (i.e., disconnected) by means of automatic protective equipment so as to avoid costly damages to the system. Subsequently, the load that was carried by line i before failure will be redistributed to remaining lines, which in turn may cause further failures, possibly leading to a *cascade* of failures.

With these in mind, an important goal is to understand the robustness of systems under the equal load redistribution model described above against *random* and *targeted* attacks. With the case of random attacks being well-understood in Chapter 3, we shift our attention in this section to understanding the vulnerability of flow-carrying networks under *targeted* attacks. As before, the main goal would be to derive design strategies (in the form of optimal load-'free

space' distributions) that would lead to maximum robustness, this time against a knowledgable adversary attacking a carefully selected set of lines. However, for this optimization problem to be well-defined one has to have a good understanding of the problem from an adversary's perspective. With this in mind, this section aims to develop *good* attack strategies that lead to maximal damage to the system for a given number of lines that can be attacked. The solution to the optimal attack problem will also help a system designer by i) revealing the worst-case attack vulnerability of the system which can help evaluate a given system design; and ii) revealing the most vulnerable lines in the system that will potentially be targeted by adversaries; this may then provide useful design guidelines for *improving* system robustness.

Formally, we consider the following optimization problem. Given N lines with loads $L_1, \ldots, L_N$ and free spaces $S_1, \ldots, S_N$, we seek to find the optimal set A of k lines that the adversary should attack in order to minimize the final fraction $n_\infty(A)$ of alive lines. We provide optimal solutions via greedy algorithms in three special cases: i) when all lines have the same load; ii) when $S_i = \alpha L_i$ for each $i = 1, \ldots, N$ (as commonly used in the literature [38, 59, 77, 84, 85, 88]); and iii) when all lines have the same free space, i.e., when $S_1 = \cdots = S_N$.

We also consider a variation of the problem with an additional constraint on the total load of the lines attacked; i.e., when the adversary is further constrained with $\sum_{i \in A} L_i \leq Q$ for some Q. From a practical point of view, this might be the case if high-load carrying lines are *protected* better by the network owner and the *cost* of attacking them is proportional to their load. We show that this variation of the optimal attack problem is in fact NP-Hard, meaning that no polynomial-time algorithm can find the set A that minimizes $n_\infty(A)$, unless $P \equiv NP$. For the modified optimization problem, we develop several heuristic algorithms and evaluate their performance in comparison with benchmarks through an extensive simulation study. In particular, we modify the previously developed heuristics with a *switch* that, when actuated during a sequential selection of lines to be attacked, changes the way algorithm makes the remaining selections; this idea is inspired from heuristics developed in [89] for the multi-

dimensional 0-1 Knapsack problem. Among other things, we demonstrate via simulations that the max-$L * S$ algorithm with a *switch* performs well in a range of settings.

4.2 Model definitions and the optimal attack problem

The load-redistribution model used here in the flow-carrying network under targeted attacks is the same as we described in Chapter 3, and the main results still hold for random attacks. Under the targeted attacks, we consider a scenario where the adversary has full information about the system and aims to find the best set of k of lines to attack so that it fails maximum number of lines as a result cascading failures. This optimization problem is formally as follows.

4.2.1 The main optimization problem: ER-k

The Equal Redistribution (ER) problem with k attacks is the *optimization problem*, denoted ER-k, that aims to find the set A of k lines such that attacking A leads to the maximum number of total line failures (as a result of load redistribution and cascading failures), among all possible attack sets with size k. Put differently, we seek to find A with $|A| = k$ that minimizes $n_\infty(A)$. Throughout, we find it useful to consider the *decision* version of this optimization problem (referred to as the ER-k-k' problem) formally defined as follows.

INPUT: N pairs of non-negative numbers in the form (L_i, C_i) indicating the load and the capacity of each line, and integers k and k' such that $0 < k < k' \leq N$. We assume $C_i > L_i$ so that no line fails initially at its own load.

OUTPUT: The answer to whether or not there is an attack set A with size k, such that at the end of the cascading failures the number of failed nodes is at least k'; i.e., whether there exists A with $|A| = k$ and $n_\infty(A) \leq N - k'$.

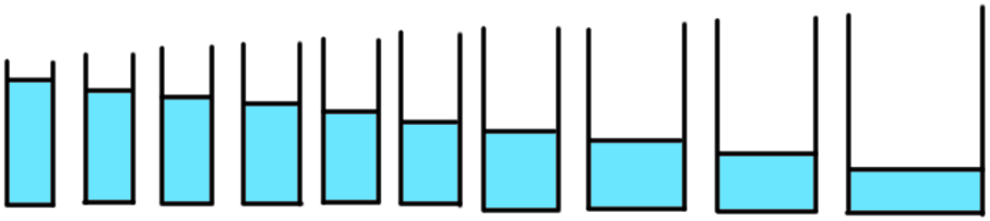


Figure 4.1: *In this example we have (load, capacity) values given by* $(10, 10 + 1/10), (9, 9 + 10/9 + \epsilon), (8, 8 + 19/8 + \epsilon), (7, 7 + 27/7 + \epsilon), (6, 6 + 34/6 + \epsilon), (5, 5 + 40/5 + \epsilon), (4, 4 + 45/4 + \epsilon), (3, 3 + 49/3 + \epsilon), (2, 52/2 + \epsilon), (1, 1 + 54/1 + \epsilon)$ *where* $\epsilon > 0$ *is arbitrarily small. The greedy maximum-load attack will need to attack* $k = 10$ *containers to fail all. It will start attacking the leftmost container with load* $L_1 = 10$ *which will not lead to any further failures. Then, it will continue with the second one from the left, again unable to trigger a cascade, and continue until attacking all containers directly. The optimal solution can be seen to be* $k = 1$ *by attacking the last container, which will trigger a cascading failure destroying the whole system. We can generalize this counterexample to the case with* N *containers with the greedy algorithm's output being* $k = N$ *while the optimal solution being* $k = 1$.

4.2.2 Heuristic algorithms that fail

Here we will present three intuitive greedy algorithms and give concrete examples demonstrating their poor performance for the optimization problem described above. In doing so, we will focus on the special case where $k' = N$ meaning that the goal of the attack is to destroy the whole system, by attacking a minimum number k of lines.

In what follows, we find it useful to describe the problem in a simpler way, where we have N water containers with capacities $C_1, \ldots, C_N$, and initial water levels $L_1, \ldots, L_N$. As in the equal flow-redistribution model, when a container is "attacked" its content is redistributed equally to the remaining containers. Also, if the water level in a container exceeds its capacity, we assume that it has failed and redistribute its content, again equally, to the remaining containers. With this formulation, the goal of the attackers is to find the smallest number k of containers to target so that all containers get overloaded and fail eventually. An important observation is that the following intuitive algorithms can deviate significantly from the optimal solution.

Greedy max-load attack. This greedy strategy aims to maximize the load that will be redistributed in each attack round. Namely, it starts by attacking the container with the highest load, and proceeds similarly, waiting after every attack for a steady-state to be reached

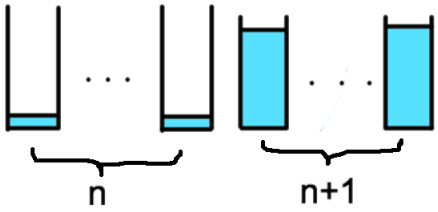


Figure 4.2: *Consider $2n+1$ containers where (load, capacity) values are given by (ϵ, M) for the first n containers and $(M-2\epsilon, M-\epsilon)$ for the last $n+1$ containers; here $\epsilon > 0$ is arbitrarily small and $M > 2(n+1)\epsilon$. The greedy max-capacity attack will need to attack $k = n+1$ containers to fail the all containers; it will start attacking the first n containers but cascading failures will not take place. On the other hand, the optimal solution is $k = 1$ as it takes to attack only one of the containers with $(M-2\epsilon, M-\epsilon)$ to trigger a cascading failure that will fail all.*

(meaning that all load redistribution and potential further failures end). The algorithm stops when all containers fail. This strategy is not optimal in general because it fails to recognize the opportunity to eliminate containers with very large capacities that will otherwise be difficult to fail by redistributing the load. The worst-case deviation from the optimal (in terms of the number of lines needed to be attacked for complete system failure) is $\Theta(n)$; e.g., see Figure 4.1.

Greedy max-capacity attack. This strategy is similar in spirit with the greedy max-load attack except that this time the container with the maximum capacity is attacked in each round. The idea here is that by taking out large containers, the remaining, supposedly small, containers will be destroyed due to load redistribution. This strategy is not in general optimal either, because there may be containers with *large* capacities but small (or, even almost zero) loads, rendering an attack to such containers very ineffective in terms of triggering failures by means of load redistribution. The worst-case deviation from the optimal is again $\Theta(N)$ as demonstrated in Figure 4.2.

Greedy max-free-space attack. It is clear from the previous two cases that the optimal attack strategy will be one that considers both the loads and capacities of the containers involved. The greedy approach that targets containers with largest free space (i.e., (*capacity* $-$

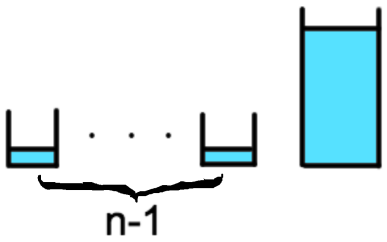


Figure 4.3: *In this example we have n containers with (load, capacity) values $(\epsilon, (n+1)\epsilon)$ for the first $n-1$ containers and $(M, M+(n-1)\epsilon)$ for the last container, where $\epsilon > 0$ is arbitrarily small and M satisfies $M > (n^2 - n)\epsilon$. The greedy max free-space $(C - L)$ attack will output $k = n$ since it will start attacking the leftmost containers and no cascading failures will take place. The optimal solution is obviously $k = 1$ by attacking the last container.*

load) difference) falls into this category, and is based on the fact that containers with largest free space will fail the *latest* in the course of a cascading failure; e.g., see Section 4.2.3 for a discussion of this fact. Therefore, it is sensible to eliminate those containers with a direct attack. On the other hand, containers with small free space are already on the verge of failing and therefore can be taken down by means of redistribution of loads. Although this greedy strategy is intuitive (and in fact optimal in some special cases), it fails to be the optimal solution in general. The main reason is that this approach does not take into account the loads of the containers directly. For example, a container may have a large free space but its load may be negligible compared to other containers, rendering a direct attack on this container ineffective. The worst-case deviation from the optimal is again $\Theta(N)$ as demonstrated in Figure 4.3.

4.2.3 Observations towards designing a smart algorithm

We now present some observations that will be useful in designing a *smart* attack algorithm.

The order of attack does not matter. In the equal redistribution model, the order with which we launch an attack does not affect the final set of failed containers. This is because the load of the attacked nodes will be distributed to all of the remaining nodes so at the end an amount of $\sum_{i \in A} L_i$ will end up in the remaining containers (leading to new failures or not) irrespective of the order we chose to attack the containers in A. We remark that an attack strategy can still be designed in a greedy fashion, where the set A is determined one member at a time, waiting for cascades to stop after each attack.

Order of failures during the cascading process. Assume that containers are sorted by increasing free space, $S_i = (C_i - L_i)$. Given that any failed load is redistributed *equally* among the remaining containers, it is clear that this ordering will remain the same throughout the course of cascading failures; the containers that are attacked directly at the beginning are excluded from this argument. Therefore, in the process of recursive load redistribution, containers will fail (due to their free space diminishing to (below) zero) in this exact same order: the one with smallest free space will fail first, and so on and so forth.

4.3 Optimal attack strategies under special cases

We now present three special cases of the ER-k problem and provide *optimal* attack strategies for each of them.

Same Loads. An interesting situation arises when initial loads are the same for all containers while capacities differ. This reflects situations in which all lines in the power system are given the same initial load, but have different capacities owing to the physical constraints or material used. We show that a greedy algorithm finds the optimal solution in this special case. The ER-k-Same Loads Problem is defined formally as follows.

INPUT: A non-negative rational number L for the common load and a list of N non-negative numbers $C_i > L, \forall i$ indicating the capacity of each line. The integer k represents the number of attacks we can launch.

OUTPUT: The set A of lines to be attacked that minimizes $n_\infty(A)$ under the constraint $|A| = k$.

The next result, proved in the Appendix, shows that the max-C-greedy algorithm finds the optimal solution.

Theorem 1. *The max-C-Greedy Algorithm is optimal for the ER-k-Same Loads Problem.*

Same Free Spaces. Sometimes it might be the case that the containers have arbitrary load and capacity but they have a fixed free space. In [90], this was in fact shown to be the optimal design that gives maximum robustness against *random* attacks. We refer to the corresponding problem as the ER-k-Same Free Spaces, formally defined as follows.

INPUT: A list of N non-negative rational numbers L_i indicating the load of each container and a positive rational number S indicating the common free space.

OUTPUT: Find the minimum number k of containers needed to be attacked in order to destroy the whole system.

We changed the output here from having a fixed number of lines to be attacked to inflict the maximum damage, to the case where we aim to destroy the whole system with the minimum number of attacks. This is because in the case where every container has the same free space, there are no intermediate cascading failures. After an attack, the system will either fail completely, or no single line will fail other than those attacked directly. We show in Appendix that the *max-L*-Greedy algorithm that targets lines with the largest loads leads to the optimal solution for this problem.

Theorem 2. *The max-L-Greedy Algorithm is optimal for the ER-k-Same Free Spaces Problem.*

Capacities Proportional to Loads. In many cases, the capacities and the loads of power lines are related in a particular way. Namely, the capacity of a line is often set to be proportional to its load. For example with $\alpha > 0$ denoting the *tolerance factor*, we have $C_i = (1 + \alpha)L_i$ for each line $i = 1, \ldots, N$. In this variation, we will also show that there is a greedy algorithm achieving the optimal solution. The ER-k-$(C \propto L)$ Problem is defined formally as follows.

INPUT: A list of N non-negative numbers L_i indicating the load of each container and a positive number α such that container capacities are set to $C_i = (1 + \alpha)L_i$ for each i.

OUTPUT: The set A of lines to be attacked that minimizes $n_\infty(A)$ under the constraint $|A| = k$.

In this setting, load, free-space, and capacity of the lines will be ordered in the same way, and as we show in the Appendix, $max\text{-}L, C, S$-Greedy algorithms that target lines with the largest load *and* free-space *and* capacity give the optimal solution to this problem.

Theorem 3. *The $max\text{-}L, C, S$-Greedy Algorithms are optimal for the ER-k-$(C \propto L)$ Problem.*

4.4 A modified optimal attack problem with total load constraints

In this Section, we will prove that a variation of the decision problem ER-k-k' is NP-Complete. In particular, we consider the ER-k-k'-Q problem, defined formally as follows.

INPUT: N pairs of non-negative numbers in the form (L_i, C_i) indicating the load and the capacity of each line, integers k and k' such that $0 < k < k' \leq N$, and a positive number Q. We also assume $C_i > L_i$ for each $i = 1, \ldots, N$.

OUTPUT: The answer to whether or not there is an attack set A with size k, and total sum of loads $\sum_{i \in A} L_i \leq Q$, such that at the end of the cascading failures the number of failed nodes is at least k'; i.e., whether there exists $A \subset \{1, \ldots, N\}$ with $|A| = k$, $\sum_{i \in A} L_i \leq Q$, and $n_\infty(A) \leq N - k'$.

It is clear that the objective is two-fold here and that there is an inherent trade-off: by attacking lines with larger initial loads we can shed more load on other lines and have a better chance to trigger a cascade of failures that would destroy the whole system. However, the problem enforces a constraint on the total load of the attacked containers as well. This *knapsack-like* trade-off is what makes the problem NP-complete as we now show. Our proof is based on the reduction of the ER-k-k'-Q problem from the *k-Subset Sum* variant defined as follows: *Given a set of integers and a target sum Q, is there any subset of size k whose sum is Q?*

Theorem 4. *The ER-k-k'-Q Problem is NP-Complete.*

Proof. First, we show that ER-k-k'-Q Problem is in NP: The certificate is a list of the k containers we choose to attack. We can check in polynomial time (e.g., see the ER-Attack Projection algorithm in [91]) whether at least k' lines in the system fail or not. Since we have a certificate that can be checked in polynomial time, ER-k-k'-Q is in NP!

Given an instance of the k-Subset Sum problem we will create an instance of the ER-k-k'-Q problem: Given a set of N integers $a_1, a_2, ..., a_N$, the k-Subset Sum problem asks whether there exists k members of the set whose some equals Q. If $k = N$, we can check if $\sum_{i=1}^{N} a_i = Q$ and respond accordingly. From now on, we suppose $k < N$ and create an equivalent version of the ER-k-k'-Q problem in the following manner. Let lines $\mathcal{L}_1, \ldots, \mathcal{L}_N$ have loads $L_1 = a_1, L_2 = a_2, ..., L_n = a_N$ and consider the ER-k-k'-Q problem; i.e., we seek to find a set A of k lines such that $\sum_{i\in A} L_i \leq Q$ and that attacking A leads to failure of at least $k' > k$ lines in the system. We also set $C_i = L_i + S_i$ where the free space is $S_i = \frac{Q}{N-k}$ for each $i = 1, \ldots, N$. This last constraint ensures two things. First, as discussed in Section 4.3, when all lines have the same free space then attacking k lines can only have two consequences: either only those k lines that are attacked fail, or all N lines fail. In either case, there is no *cascade* of failures and the system reaches a steady-state immediately. Thus, with equal free space among all lines, the ER-k-k'-Q problem with $k' > k$ is equivalent to ER-k-N-Q problem. Secondly, under the enforced assumptions it is clear that a complete system failure will take place if and only if the total load failed by the initial attack A is larger than the sum of the free spaces of those that are not in the attack set A; i.e., if and only if

$$\sum_{i\in A} L_i \geq \sum_{j\in\{1,\ldots,N\}/A} S_j = (N-k)\frac{Q}{N-k} = Q.$$

Here, the first equality follows from the facts that $|A| = k$ and $S_i = \frac{Q}{N-k}$ for each $i = 1, \ldots, N$. Recalling further the constraint that $\sum_{i\in A} L_i \leq Q$, this leads to $\sum_{i\in A} L_i = Q$. Therefore, the created instance of the ER-k-k'-Q problem indeed seeks to find a subset A of $\{a_1, \ldots, a_N\}$

such that $|A| = k$ and $\sum_{i \in A} L_i = Q$, rendering it equivalent to the k-Subset Sum instance that we have started with. For the reverse direction, assume that the ER-k-k'-Q problem has a solution with k lines $\mathcal{L}^{(1)}, \ldots, \mathcal{L}^{(k)}$. Then the loads of these lines constitute a solution to the k-Subset-Sum problem.

The above reduction can be constructed in polynomial time (more precisely, in linear time), so if there was a polynomial algorithm that could solve the ER-k-k'-Q, then the k-Subset Sum would be in P, which is wrong unless P=NP. Thus, we conclude that the ER-k-k'-Q Problem is NP-complete. ■

An important implication of the above result is that the *optimization* version of the ER-k-k'-Q problem, which seeks to find the set A of lines that minimizes $n_\infty(A)$ under the constraints $|A| = k$ and $\sum_{i \in A} L_i \leq Q$, is NP-Hard. This means that under these constraints, the adversary can not launch an optimal attack in polynomial time unless P=NP.

4.5 Heuristic algorithms and their performance

Although, it is not known whether the original optimization problem of finding the best k lines to attack to minimize final system size is NP-Hard or not, the discussion in the preceding section indicates that the optimal attack problem is likely to be computationally challenging; in particular, we know that the problem is NP-Hard if we are further constrained by the total load of those we can attack. This prompts us to develop heuristic algorithms, for both the original and the modified optimization problems, that work in polynomial time and have competitive performance under arbitrary load-capacity distributions. The performance of these heuristics will then be compared with some benchmark heuristics such as max-L, max-C, max-S, and random attacks.

In the interest of brevity and concreteness, the discussion is restricted here to *non-greedy* algorithms that choose the attack set A *without* ever running the attack projection algorithm.

In other words, the algorithms are not allowed to run the cascading failures initiated by a subset of A, and then continue making the remaining selections from the lines that survived the cascade. Of course, all heuristics considered here including the benchmarks can be modified to operate in a greedy fashion. One might also be tempted to use a greedy algorithm where, at each round, the line to be attacked is chosen in an optimal way; i.e., the line whose failure leads to smallest number of surviving lines is chosen from among all lines that are still alive. However, for the problem at hand, one can realize that unless $|A|$ is relatively large, the final system size equals $n_\infty(A) = N - |A|$ regardless of the set A of attacked lines. For example, with $|A| = k$, this will be the case whenever

$$k \leq \frac{S_{min}}{L_{max}}(N - k),$$

meaning that if $S_{min}/L_{max} > 0$, the greedy heuristic will have to deal with *ties* when making its choices for the next line to be attacked until it makes $\Omega(n)$ choices. Since resolving the ties by randomization for such a large number of selections is likely to lead to poor performance, one needs heuristic rules to resolve the ties. Even then, our preliminary simulation study indicated that the greedy versions of the heuristics considered here perform only slightly better than their non-greedy counterparts, and the comparison among the greedy heuristics provided no additional insight to what was already observed from non-greedy algorithms; hence the decision to consider only non-greedy attack strategies here.

4.5.1 Heuristics for the original optimization problem

We first consider the original case where there is no constraint on the total load of the lines that can be attacked; i.e., we consider the ER-k problem. Let A be the set of lines to be attacked such that $|A| = k$. It is clear from the previous discussions that a good attack should

aim to

$$\text{maximize} \sum_{i \in A} L_i, \quad \text{and} \tag{4.1}$$

$$\text{minimize } S_j, \ j \in \{1, \ldots, N\} - A \tag{4.2}$$

In words, the attack should aim to find the lines with the largest free space while making the total load of the failed lines as large as possible. Thus, the attack should intuitively look for lines with *large* initial load *and large* free-space. Of course, most difficult situations arise when the load and free-space values of the lines are in reverse order; e.g., the highest load carrying line has the smallest free-space, etc. as in Figure 4.1.

Our main idea towards handling the trade-off described above is based on its similarities with the well-studied 0-1 Knapsack problem. In the 0-1 Knapsack problem, we are given a set of N items, $\{1, \ldots, N\}$, each with a weight w_i and a value v_i, and the goal is to choose items such that their total value is maximized while the total weight is bounded by W; i.e.,

$$\text{maximize} \sum_i v_i x_i \tag{4.3}$$

$$\text{subject to} \sum_i w_i x_i \leq W \quad \text{and} \quad x_i \in \{0, 1\} \tag{4.4}$$

The 0-1 Knapsack problem is known to be NP-Hard, but polynomial-time heuristics can still give close-to-optimal solutions. For example, a competitive heuristic is to order the items based on their "value per weight", i.e., v_i/w_i, and choose items according to this order, starting with the one with the highest v_i/w_i, until the total weight capacity W is reached. In fact, with a small modification to handle corner cases, this heuristic is known to yield at least 50% of the optimum value.

The optimal attack problem we consider, i.e., the ER-k problem, has some similarities with but is not equivalent to the 0-1 Knapsack problem. In particular, one can construct an analogy between the constraints of the 0-1 Knapsack problem and the ER-k problem by assigning all

item weights as $w_i = 1$ and the total weight limit to be $W = k$. However, the objectives (4.1)-(4.2) of the ER-k problem are much more complex than the objective (4.3) of the Knapsack problem. Nevertheless, the two problems have some similarity in that their main difficulties lie in the trade-offs involved. In the Knapsack problem the trade-off is between the value and the weight of the item and it is desirable to pick items with high value and low weight, while in the ER-k, the trade-off lies between the possibly conflicting objectives of choosing lines with high load and high free-space. Inspired with the efficient heuristic for the Knapsack problem that is based on selecting items with the largest v_i/w_i ratio (i.e., items with the biggest *bang for the buck*), our first heuristic for the ER-k problem is based choosing lines with the highest load times free-space, i.e., with the highest $L_i * S_i$.

Maximum Load×Free Space Attack. In this algorithm, the load free space product, $L_i * S_i$ is computed for each line $i = 1, \ldots, N$. After sorting the lines based on this product, the k lines to be attacked is chosen as the ones having the highest k load-free space product. As mentioned above, this is inspired by the 2-approximation heuristic for the Knapsack problem that orders items according to $v_i * \frac{1}{w_i}$ when the goal is to choose items with high v and low w. In the ER-k problem, we wish to choose lines with high L and high S, or equivalently, with high L and low $\frac{1}{S}$. Thus, constructing an analogy between value v_i and load L_i, and weight (or, cost) w_i and $1/S_i$, our heuristic chooses lines with the maximum

$$L_i * \frac{1}{1/S_i} = L_i * S_i.$$

The performance of this heuristic is demonstrated via several numerical examples in the next subsection along with a comparison with some benchmark heuristics.

Aside from its connection to a powerful heuristic in a relevant problem, the maximum $L * S$ heuristic has several advantages. First of all, this heuristic becomes equivalent to the *optimal* attack strategy in the three special cases considered in Section 4.3; e.g., when all lines have the same load, it chooses ones with highest free-space (and hence capacity), or when all lines

have the same free-space, it chooses lines with maximum L, etc. Secondly, considering the product $L * S$ is an effective way to favor lines with high load *and* free-space, while heavily penalizing load or free-space values close to zero; note that benchmark heuristics including the highest-capacity attack ($C = L + S$) fail to penalize small L or C values. In the optimal attack problem, this makes perfect sense given that a line with almost no load should never be attacked even if it has very high free-space since its failure will likely not affect any other line. Similarly, it may not be a good idea to directly attack a line with almost no free-space even if it has very high load, since the line will likely fail due to load redistribution *regardless* of which other lines are attacked.

Maximum $L * S^{\beta}$ attack. While maximum $L * S$ attack is intuitive and will be seen to be powerful in many cases, we observe that its performance can be further improved by a small modification. To this end, we propose a second heuristic as a modified version of the max-$L*S$ attack that allows adjusting the relative importance of load and free-space values of the lines. In particular, with β in $[0, \infty]$, we consider a heuristic that chooses k lines with the maximum $L_i * S_i^{\beta}$. An added benefit of this heuristic is that it contains several heuristics as special cases. In particular, the maximum $L * S$ algorithm described above is obviously a special case of this algorithm, corresponding to the case $\beta = 1$. Also, by setting $\beta = 0$, this heuristic reduces to the max-L attack, while setting $\beta = \infty$ (or, large enough) makes it equal to the max-S attack.

4.5.2 Numerical comparison with benchmark heuristics

We now compare the heuristics we developed against some benchmark heuristic algorithms via numerical experiments. The benchmark heuristics we will consider are given below:

Random attack. This is the most primitive attack strategy and considered here only for comparison purposes. The attack picks k lines to be attacked uniformly at random from amongst all N lines.

Highest-L, highest-C, highest-S attacks. These three attacks are based on sorting lines with respect to their initial load L_i, free-space S_i, or capacity $C_i = L_i + S_i$, respectively and attacking the top k lines with the highest value of the corresponding metric.

We fix the number of lines at $N = 5000$ for all experiments. First, we consider the case where each line is independently given an initial load from a uniform distribution, $U(L_{min}, L_{max})$, where we set $L_{min} = 10$ and $L_{max} = 30$. The free-space allocated to each line is generated independently from its load, again from a uniform distribution, $U(S_{min}, S_{max})$ with $S_{min} = 10$, $S_{max} = 60$. The capacity of a line $\mathcal{L}_i$ is given by the sum $C_i = L_i + S_i$. The independence of L and S leads to some lines having high load but small free-space, or vice versa, rendering the optimal attack problem *non-trivial*; e.g., with these choices, the realized load-capacity values will almost surely *not* fall into one of the special cases presented in Section 4.3 where an optimal solution is available.

Under this setup, we compute the final system size as a function of the number k of lines attacked, where the set of attacked lines are selected according to the heuristics considered. The results are given in Figure 4.4 where each data point is obtained by averaging over 100 independent runs. We already see in this simple setting that our attack strategy of targeting lines with the highest $L * S$ outperforms all other benchmarks (except a small interval of attack size where max-L attack seems to give the highest damage). In particular, we see that the highest $L * S$ attack is able to fail the whole system by targeting 90, 180, 210, and 450 fewer lines as compared to max-C, max-L, max-S, and random attacks, respectively.

Next, we check if this performance can be further improved by attacking lines with highest $L * S^\beta$ for some $\beta \geq 0$. To this end, we repeat the previous experiment as β varies from zero to ten. The results are demonstrated in Figure 4.5 and as expected show that with $\beta = 0$ or $\beta \gg 1$, we obtain the same performance with max-L and max-S attack, respectively. More interestingly, we see that the case $\beta = 1$ is indeed *not* the best one can do. For example, we see that when $\beta = 0.3$, the max-$L * S^\beta$ attack can fail the whole system by attacking 75 fewer lines the case for $\beta = 1$. To demonstrate this better, we plot in the inset of Figure 4.5 the

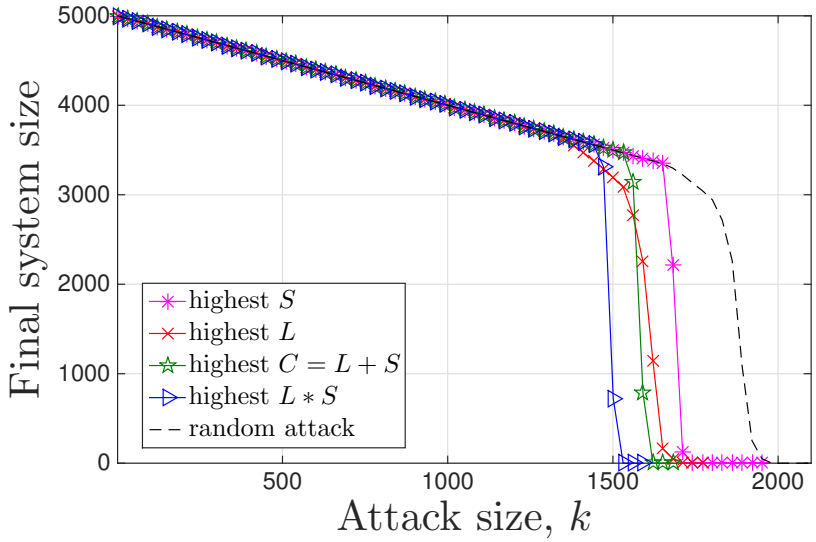


Figure 4.4: *The performance comparison of different heuristic algorithms for* $L \sim U[10, 30]$, $S \sim U[10, 60]$, $N = 5000$.

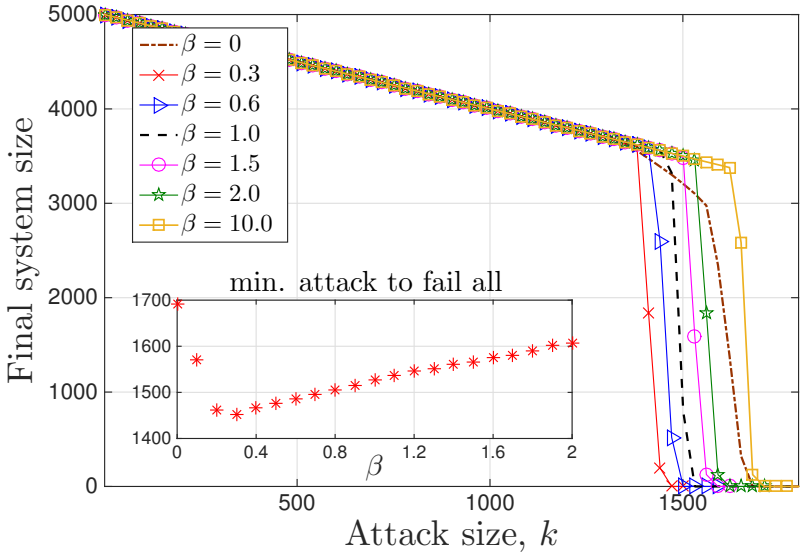


Figure 4.5: *The performance comparison of maximum* $L * S^{\beta}$ *algorithms for various* β *values for* $L \sim U[10, 30]$, $S \sim U[10, 60]$, $N = 5000$. *Inset: The minimum number of lines needed to be attacked to fail all lines for the maximum* $L * S^{\beta}$ *attack.*

minimum number lines needed to be attacked to fail all N lines. To compute this, we again run 100 independent experiments and pick the minimum attack size for which *all* 100 experiments led to entire system failure.

The performance of heuristic algorithms are known to vary significantly under different parameter settings, and our case is not expected to constitute an exception. To that end, we

have tested the performance of the max-$L * S^\beta$ attack with $\beta \in [0, 4]$, for a wide range of possibilities for the distribution of L and S. In all cases we considered, we were able to identify a β value for which the max-$L * S^\beta$ attack was at least as good as all benchmark attacks (random, highest-C, L, S-attacks) showing its versatile performance.

As already mentioned, the most challenging cases arise when the load and free-space values are in reverse order. To that end, we close this section by demonstrating the performance of the max-$L * S^\beta$ attack in such cases. In particular, we start by generating $L_1, \ldots, L_N$ and $S_1, \ldots, S_N$ independently according to some distribution. Then, the load values (resp. free-space values) are sorted and re-arranged in increasing (resp. decreasing) order, leading to highest-load carrying line having the smallest free-space, and so on. To make the problem more challenging and interesting, we also consider *Pareto* distribution. Namely, a random variable X is said to follow Pareto distribution, written $X \sim \text{Pareto}(X_{\min}, b)$ with $X_{\min} > 0$ and $b > 0$, if its probability density is given by

$$p_X(x) = X_{\min}^b b x^{-b-1} \mathbf{1}\left[x \geq X_{\min}\right].$$

To ensure that $\mathbb{E}[X] = bX_{\min}/(b-1)$ is finite, one must set $b > 1$, while the variance of X is finite only if $b > 2$.

The results for the case where L and S values are reverse ordered are depicted in Figure 4.6. Here, we show a small number of representative results that correspond to different behaviors for brevity. As before, all results correspond to the minimum attack size that led to an entire system collapse in all 100 experiments. The curves represent the results for the max-$L * S^\beta$ attack as β varies from zero to two. In each plot, we add the corresponding results for the max-C attack (shown by a filled square) and random attack (shown by a filled circle) as well; for convenience, the x-axis values for these symbols are chosen such that they stay on the corresponding curve showing the results for max-$L * S^\beta$ attack. We note that the max-L attack is already demonstrated by the case $\beta = 0$ while $\beta = 2$ gives a good indication of the performance of the max-S attack, so these plots provide a comparison of the max-$L * S^\beta$ attack

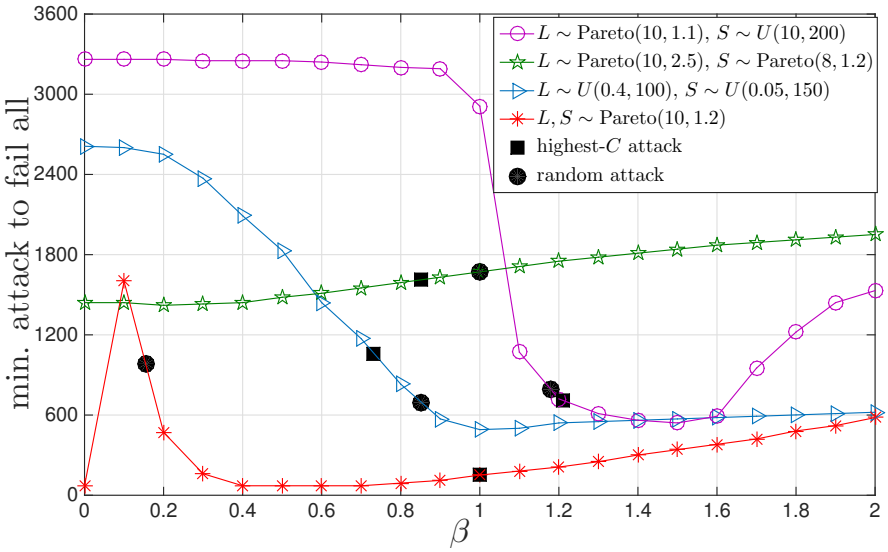


Figure 4.6: *Minimum number of lines needed to be attacked to fail all lines in the system is shown when load and free-space values are generated independently (from the distributions given at the figure legend) and then sorted in reverse orders; e.g., to ensure* $L_1 \leq L_2 \leq \cdots \leq L_N$, *while* $S_1 \geq S_2 \geq \cdots \geq S_N$. *Curves stand for the results obtained under the max-*$L * S^\beta$ *attack as a function of* β. *Corresponding results for the max-*C *attack are shown by filled square symbols, and those for the random attack by filled circles.*

with all the benchmarks considered here.

The main observations from Figure 4.6 are as follows. We see that in all cases there is a particular β value for which the max-$L * S^\beta$ attack performs the best among all benchmarks; it is only the case of $L, S \sim$ Pareto$(10, 1.2)$ where we see that the best performance of max-$L * S^\beta$ attack is attained when $\beta = 0$, or $\beta \in (0.4, 0.7)$ meaning that max-L attack matches the performance of the max-$L * S^\beta$ attack. Also, we see that the β value that leads to the best performance can be equal to, smaller than, or larger than one in different scenarios showing the importance of trying different values of β to get the best performance. Finally, while benchmark attacks (including the random attack) occasionally give results close to the best max-$L * S^\beta$ attack, we see examples for each benchmark where its performance is significantly worse than the best max-$L * S^\beta$ attack; these cases are summarized in Table I.

4.5.3 Heuristic attacks for the modified optimization problem

We now consider the modified optimization problem ER-k-k'-Q where the attack set A is further constrained by $\sum_{i\in A} L_i \leq Q$, in addition to $|A| \leq k$. As shown in Theorem 4, in this case finding the attack set A that minimizes the final system size is NP-Hard, prompting us to develop heuristic strategies. With the additional constraint on the total load of the lines that we can attack, the trade-offs involved become more complicated and heuristics developed in the previous section may not be well-suited for the ER-k-k'-Q problem. Ultimately, our strategy should be to choose an attack set that has k (or, very close to k) lines with total load equal (or, very close) to Q, and that have the highest free space among all lines. This is because at the first stage of the cascades, any line $\mathcal{L}_i$ that was not directly attacked will fail only if

$$S_i \leq \frac{\sum_{i\in A} L_i}{N - |A|}.$$

Thus, to facilitate failures it is desirable to make $\sum_{i\in A} L_i$ and $|A|$ as large as possible, while S_i as small as possible.

Distribution of L and S	Minimum # of lines to attack to fail all				
	random	max-C	max-L	max-S	best β
$L \sim$ Pareto$(10, 1.2)$ $S \sim$ Pareto$(10, 1.2)$	**981**	**151**	71	**2241**	71
$L \sim U(0.4, 100)$ $S \sim U(0.05, 150)$	691	**1061**	**2611**	**1021**	491
$L \sim$ Pareto$(10, 2.5)$ $S \sim$ Pareto$(8, 1.2)$	1671	1611	1421	2111	1411
$L \sim$ Pareto$(10, 1.1)$ $S \sim U(10, 200)$	**791**	711	**3261**	**2221**	541
L, S from the UK National Grid*	**2371**	1491	1611	**2111**	1441

Table 4.1: *Performance comparison of benchmark attacks with the best result of the max-$L * S^\beta$ attack. The first four rows are obtained from Figure 4.6, while the last row is obtained from simulations with UK National Grid data (see Section 4.6 for details). Values significantly worse (in the sense of needing to attack many more lines to fail all) than the best-$L * S^\beta$ attack are made bold.*

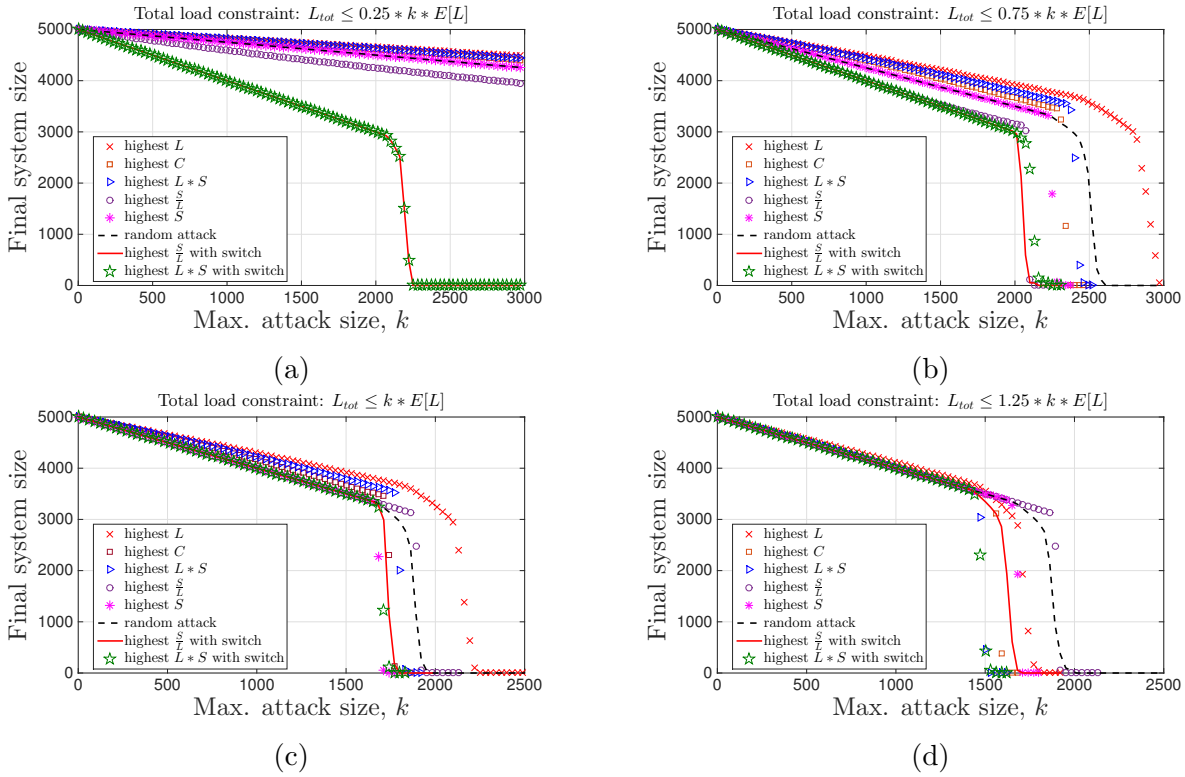


Figure 4.7: *The performance comparison of different heuristic algorithms for* $L \sim U[10, 30]$, $S \sim U[10, 60]$, $N = 5000$, *when the attack is constrained to* k *lines such that their total load satisfies a)* $L_{tot} \leq 0.25 * k * \mathbb{E}[L]$; *b)* $L_{tot} \leq 0.75 * k * \mathbb{E}[L]$; *c)* $L_{tot} \leq 1.0 * k * \mathbb{E}[L]$; *d)* $L_{tot} \leq 1.25 * k * \mathbb{E}[L]$.

Given the multiple constraints involved, this problems shows similarity with the *2-dimensional 0-1 Knapsack problem* [89, 92, 93]: Consider a collection of items, where each item i is given a value v_i, has weight w_i, and volume q_i. The objective is then to maximize $\sum_i v_i x_i$ subject to $\sum_i w_i x_i \leq W$ *and* $\sum_i q_i x_i \leq Q$ where $x_i \in \{0, 1\}$; i.e., we want to choose items with the maximum total value while the total weight is limited by W and total volume is limited by Q. As can be inferred from the discussion above, an important difference of the ER-k-k'-Q problem is that while it is desirable to choose lines with high S_i (could be thought to be analogous to the "value" of the item) under given constraints, it is perhaps equally important to attain or be very close to the limits on both total load and total number of lines attacked.

With these in mind, our heuristics for the ER-k-k'-Q problem are based on incorporating a *switch* to the previously developed heuristics that is actuated to ensure that the attack set A attains or gets close to both constraints on its cardinality and the total load. This idea is

inspired from the greedy-like heuristic developed for the multi-dimensional Knapsack problem in [89]. This algorithm initially starts choosing items based on a given set of rules until one or more of the constrained resources become scarce, and then switches to a different set of rules that favor items that use very little of the scarce resource. Here, we propose to use a heuristic that chooses the lines to be attacked one at a time according to the previously developed max-$L * S$ strategy. After each selection, we check whether the switch needs to be activated. Namely, with A' denoting the set of k' lines selected so far, we check

i) Is it still feasible to select all remaining $k - k'$ lines from the smallest load carrying lines available? Namely, with the remaining lines' loads sorted in ascending order $L^{(1)} \leq L^{(2)} \leq \cdots \leq L^{(N-k')}$, we check if

$$\sum_{j=1}^{k-k'} L^{(j)} + \sum_{i \in A'} L_i \leq^{?} Q$$

If the answer is YES, we continue with the second condition for the switch, while if the answer is NO, the switch is activated and algorithm is finished by appending A' with $k-k'-1$ lines with the smallest load-carrying lines available; i.e., with $\mathcal{L}^{(1)}, \ldots \mathcal{L}^{(k-k'-1)}$. Alternatively, one can release the latest added member of A' and append it with $k-k'$ lines $\mathcal{L}^{(1)}, \ldots \mathcal{L}^{(k-k')}$; we found no major performance difference between these two approaches.

ii) Next, check whether it is feasible to select all remaining $k - k'$ lines from the largest load carrying lines available. Namely, with the remaining lines' loads sorted in ascending order $L^{(1)} \leq L^{(2)} \leq \cdots \leq L^{(N-k')}$, we check if

$$\sum_{N-k+1}^{N-k'} L^{(j)} + \sum_{i \in A'} L_i \leq^{?} Q$$

If the answer is NO, we continue the algorithm with the next selection, while if the answer is YES, the switch is activated and algorithm is finished by appending A' with $k - k'$ lines with the largest load-carrying lines available; i.e., with $\mathcal{L}^{(1)}, \ldots \mathcal{L}^{(k-k'-1)}$.

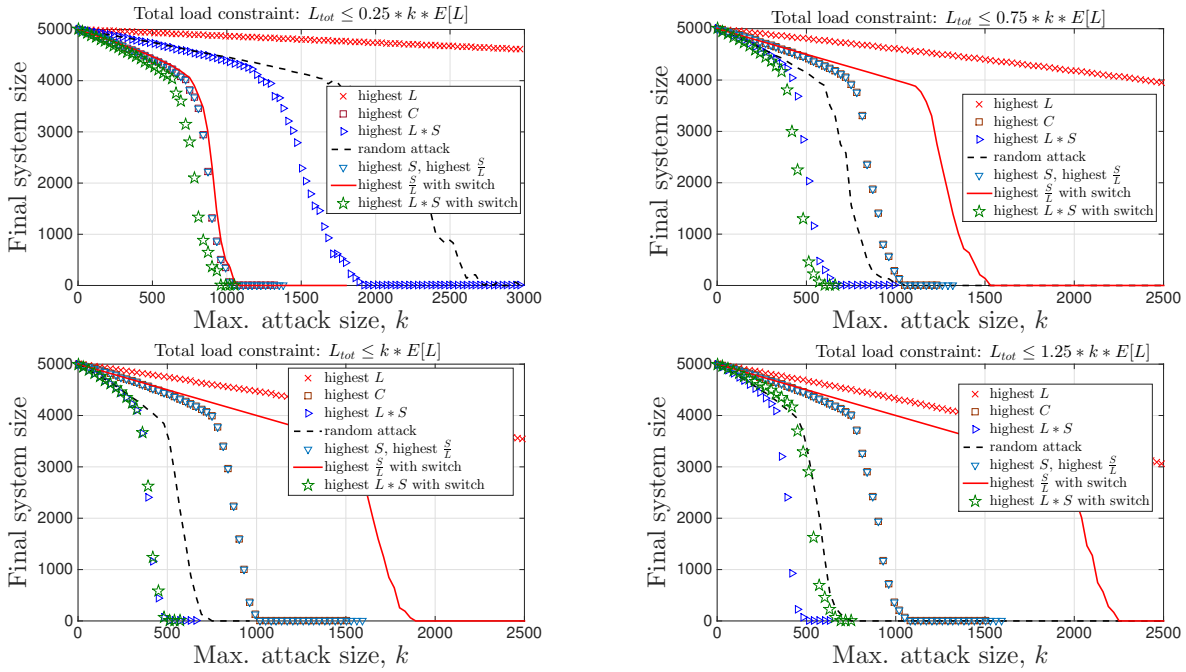


Figure 4.8: *The performance comparison of different heuristic algorithms for* $L \sim U[0.4, 100]$, $S \sim U[0.05, 150]$, *with* L *and* S *sorted in reverse order,* $N = 5000$, *when the attack is constrained to* k *lines such that their total load satisfies a)* $L_{tot} \leq 0.25 * k * \mathbb{E}[L]$; *b)* $L_{tot} \leq 0.75 * k * \mathbb{E}[L]$; *c)* $L_{tot} \leq 1.0 * k * \mathbb{E}[L]$; *d)* $L_{tot} \leq 1.25 * k * \mathbb{E}[L]$. *Each data point is obtained by averaging over 100 independent runs.*

The two conditions of the switch described above ensure that while the initial selections are made in line with the original objectives of picking lines with high load and high free-space, care is also given so as to be able to pick k (or, $k-1$) lines whose total load is close to the limit Q. Of course, any algorithm including the benchmarks can be modified using the switch idea to better accommodate total load constraints. In particular, when the total load limit Q is extremely stringent, it would be tempting to pick lines with small load so as to not exhaust the total load limit quickly, while aiming to choose lines with high free-space. This prompts us to consider the max-S/L heuristic as well, including its modification with the *switch* idea described above. To keep the discussion brief we do not present results for the max-$L * S^{\beta}$ attack (with or without switch) and consider only the case where $\beta = 1$; this is in part due to the fact that when the switch is added, the performance of the max-$L * S^{\beta}$ attack becomes much less sensitive to variations in β over small ranges.

We now present numerical results to evaluate the performance of the heuristic attacks

developed here and compare them against benchmark algorithms; as before, we will use max-C, S, L and random attacks as benchmarks. Different from the experiments conducted in Section 4.5.1, here we have to vary not only the maximum number k of lines that can be attacked, but also the limit Q on the total load of the attacked lines. In particular, we would expect the performance of the algorithms to depend heavily on Q. To this end, we find it meaningful to let Q vary with k and to set it in reference to the *mean* total load of k randomly selected lines; i.e., we set

$$Q = Q(k) = c * k * \mathbb{E}[L] \tag{4.5}$$

for some constant $c > 0$. This choice enables us to tune c to different levels and check performance in cases where (i) the total load is extremely limited (i.e., $c \ll 1$); ii) total load limit is such that heuristics that do not take load into account (such as max-S or random attacks) will likely be able to select (close to) k lines with total load very close to Q (i.e., $c \approx 1$); or iii) total load limit is not stringent at all (i.e., $c \gg 1$) and the problem is similar to the unconstrained load case.

In the first set of experiments, we set $N = 5000$ and generate load-free space values independently from the distributions $L \sim U[10, 30]$ and $S \sim U[10, 60]$. For brevity we consider four values of c given at (4.5): $c = 0.25$, $c = 0.75$, $c = 1.0$, $c = 1.25$. The results are presented in Figure 4.7 from which a number of interesting observations can be made. When $c = 0.25$, i.e., when total load is extremely constrained, we see that all heuristics without a switch perform poorly and are not able to fail the whole system even until $k = 3000$. This can be attributed to their inability to attack the maximum allowed number k of lines as they quickly exhaust the total load limit. On the other hand, we see that both max-$L * S$-with-switch and max-S/L-with-switch attacks perform much better, and despite the stringent limit on the total load are able to fail the system by attacking about 50% more lines than required in the case where the total load is unlimited. When c is increased to 0.75, we see that the performance of the benchmarks improve but still are significantly worse than the two heuristics that use

the switch; in this case we also see that the max-S/L-with-switch attack slightly outperforms max-$L * S$-with-switch.

With $c = 1$, we see that algorithms that ignore the loads such as max-S and random attacks perform as well as they do in the unconstrained case; this is expected by virtue of the law of large numbers. In particular, when $c = 1$, we would expect max-S to perform well since it picks the most robust lines in the system and is likely to reach the limits k and Q simultaneously given that L is independent from S. Figure 4.7c confirms this intuition where we also see that both heuristics with switch match the performance of the max-S attack. Finally, with $c = 1.25$, we get close to the unconstrained load case, and as expected see that the performance of the max-$L * S$ algorithm becomes the best. What is interesting here is that the max-$L * S$-attack-with-switch is able to match this performance, showing its versatile performance across very different cases considered here. Overall, these experiments demonstrate that incorporating the *switch* significantly improves the performance and the max-$L * S$-attack performs well across different ranges of the total load limit.

As in Section 4.5.1, it is of interest to check the performance of these algorithms in difficult cases where load and free-space values are sorted in reverse orders. To this end, we consider one of the settings used in Figure 4.6, and generate load and free-space independently from $L \sim U[0.4, 100]$ and $S \sim U[0.05, 150]$, and then sort them in reverse orders so that the line with maximum load gets the smallest free-space and so on and so forth. In this setting, max-S and max-S/L heuristics become equivalent. Also, since large S values are around 150 while L is limited to 100, the lines with maximum-C will be those with large S (and small L due to reverse ordering). As seen in Figure 4.8, this leads to three benchmarks (max-$S, C, S/L$) performing almost equally in this setting.

We see from Figure 4.8 that the max-$L * S$-attack-with-switch once again performs well. It leads to the best performance among all heuristics considered for $c = 0.25$, $c = 0.75$, and $c = 1.0$ (equal with max-$L * S$), while coming second for $c = 1.25$ after max-$L * S$; this is expected since without a stringent limit on total load, the problem gets closer to the unconstrained case

where a switch is not needed. Also, in this case we see that the performance of the max-S attack (along with max-S/L and max-C attacks) is rather unaffected by the load constraint. We attribute this to the fact that since load and free-space are reverse ordered, targeting max-S lines is equal to targeting min-L lines and even when $c = 0.25$ the total load limit is not likely to be exhausted easily; i.e., the algorithm is able to choose k lines without exceeding the total load limit. We think this is also the reason why the *switch* is not helping (and, actually hurting) the max-S/L algorithm in this case.

4.6 Simulations with UK National Grid data

In this section, we provide simulation results illustrating how the attack strategies covered here performs when the load and free space distribution are based on real data. We have used National Grid Electricity Ten Year Statement 2016 Model of Great Britain [4] to generate load-free space pairs. To be more precise, the load distribution is chosen from the winter peak power flow diagram presented in [4, Appendix C]. For the free-space distribution, the transmission line ratings given in [4, Appendix B] has been used. As in the case of previous examples, the number of lines is taken as $N = 5000$.

In Figure 4.9, we show the performance of the heuristic algorithms for the unconstrained case, i.e., for the ER-k problem. The results are very similar to those obtained under synthetic load-free space distributions and demonstrate that heuristics developed here perform well under real-world distributions as well. In particular, we see that the proposed max-$L * S$ heuristic performs better than all benchmarks considered, and its performance can further be improved by the max-$L * S^{\beta}$ attack. For the UK National Grid data, our results indicated that the best performance is obtained when $\beta = 1.5$; see also the last row in Table I.

Next, we consider the ER-k-k'-Q problem where the total load of the attack set is bounded by Q. As in Figures 4.7 and 4.8, we set Q according to (4.5) for several c values, and compare the performance of our attack strategies with benchmarks; this time the load-free space distribution is set according to the aforementioned UK National Grid data. The results are depicted in

Figure 4.10. Once again we see that the max-$L * S$ attack *with switch* leads to the best overall performance among all heuristics considered; it leads to the best performance when $c = 0.25$ (tied with max-S/L with switch), $c = 0.75$, and $c = 1.25$, while coming as second for $c = 1$ after max-S/L. This shows that the heuristic attacks proposed here have versatile performance also under distributions observed in real-world power systems.

4.7 Proofs for the theorems

4.7.1 A proof of Theorem 1

A key observation is that since the failed load is always redistributed *equally* among *alive* lines, the system will preserve the "equal load" property through the cascading failures. Namely, at any stage the load of a line that is functioning will be given by $L(1 + \frac{M}{N-M})$ where M is the number of lines (out of N) failed thus far. In addition the sequence of attacks does not affect the final state of the system as discussed before. Therefore, the claim would follow for general attack sizes k, if we establish it for $k = 1$. This is because after a single line is attacked, the system will again be one with equal loads and the optimization problem will repeat itself with $k - 1$ additional lines to be attacked. Continuing in this manner, we see that the optimal

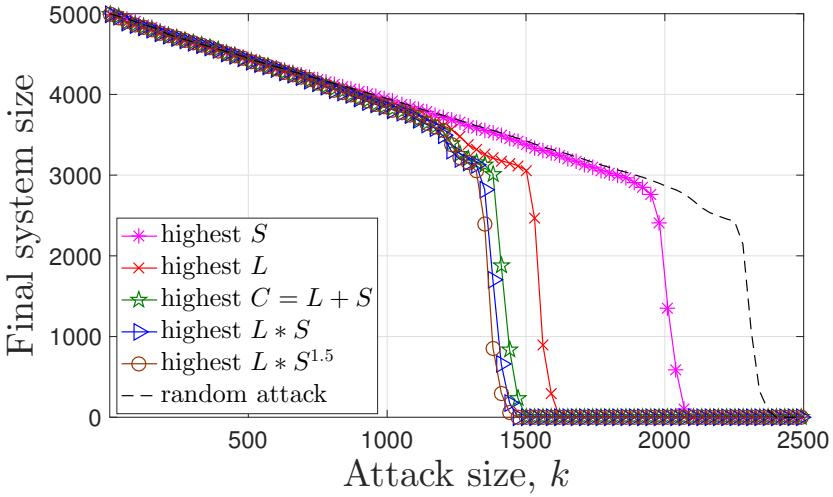


Figure 4.9: *The performance comparison of different heuristic algorithms when L, S follow the UK National Grid data [4].*

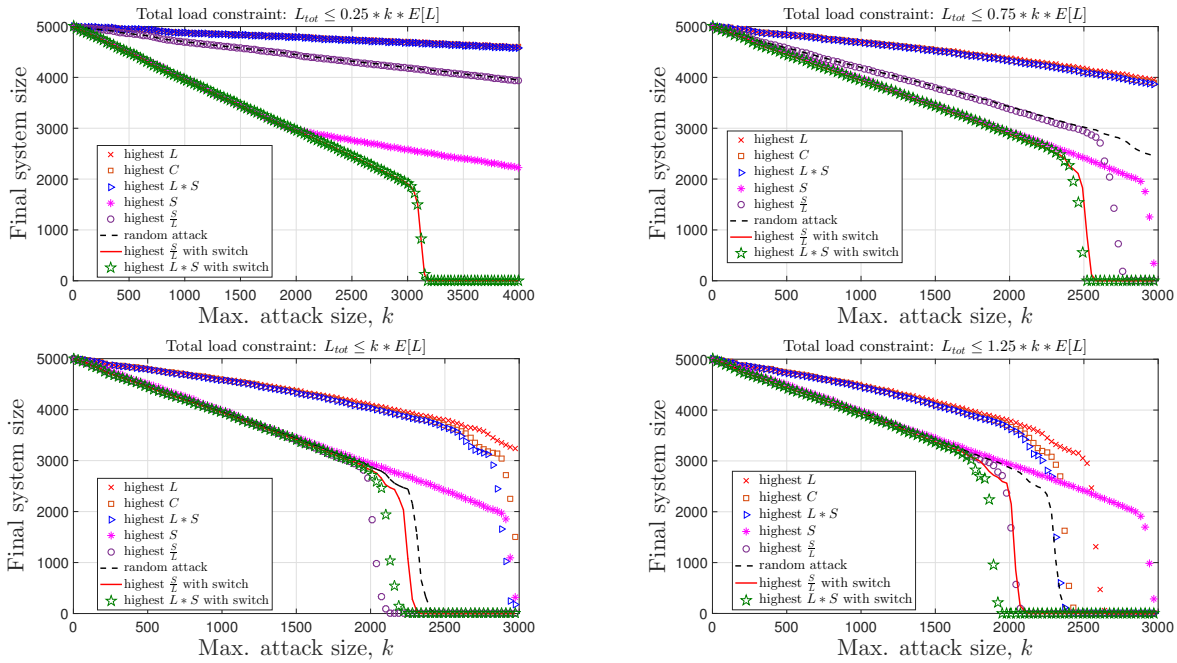


Figure 4.10: *The performance comparison of different heuristic algorithms when L, S pairs are distributed according to the UK National Grid data [4]. The attack is constrained to k lines such that their total load satisfies a) $L_{tot} \leq 0.25 * k * \mathbb{E}[L]$; b) $L_{tot} \leq 0.75 * k * \mathbb{E}[L]$; c) $L_{tot} \leq 1.0 * k * \mathbb{E}[L]$; d) $L_{tot} \leq 1.25 * k * \mathbb{E}[L]$.*

attack strategy in this case would be a combination of *optimal* single-line attacks launched sequentially.

Assume now that $k = 1$, i.e., the goal is to attack the line that will lead to the maximum number of failed lines. Since all loads are equal, the lines that fail *initially* as a result of this attack will be (with A_0 denoting the line chosen)

$$proj(A_0) := \{A_0\} \cup \left\{ \ell \in \{1, 2, \ldots, N\}/A_0 : C_\ell \leq LN/(N-1) \right\}$$

With $\mathcal{L}_i$ and $\mathcal{L}_j$ denoting arbitrary distinct lines, we have

$$|proj(\mathcal{L}_i)| - |proj(\mathcal{L}_j)| = \mathbf{1}\left[C_j \leq LN/(N-1)\right] - \mathbf{1}\left[C_i \leq LN/(N-1)\right]$$

which automatically gives $|proj(\mathcal{L}_i)| \geq |proj(\mathcal{L}_j)|$ if $C_i \geq C_j$. Since i and j are arbitrary, this

shows that

$$\arg\max_{i=1,\ldots,N} proj(\mathcal{L}_i) = \arg\max_{i=1,\ldots,N} C_i,$$

meaning that attacking the max-C line maximizes the number of lines failed initially. Also, with all loads equal, attacking the max-C line is equivalent to attacking the max-S line so this attack also collectively minimizes the free space of remaining lines. In other words, with $i^\star = \arg\max_{i=1,\ldots,N} C_i$, we have

$$\{S_\ell\}_{\ell \notin proj(\mathcal{L}_i^\star)} \leq \{S_\ell\}_{\ell \notin proj(\mathcal{L}_j)}$$

for any $j = 1, \ldots, N$ where the comparison is made pairwise. Combining, we see that the max-C attack maximizes the number of initially failed lines and minimizes the free-space of those that remain. Since all lines have equal load, this then shows that the final number of failed at the end of a potential cascade will be minimized by attacking the max-C line.

4.7.2 A proof of Theorem 2

As before, a key observation is that the optimization problem can be reduced to finding the optimal single-line attack, and repeating this recursively. The reason is that since failed load is equally redistributed, the system will maintain to have the same free space (among all alive lines) throughout the cascade process. Given also that the order of the attack does not matter, it remains to find the optimal single-line attack, i.e., the case where $k = 1$. Here, we have

$$proj(A_0) = \{A_0\} \cup \{\ell \in \{1, 2, \ldots, N\}/A_0 : S_\ell \leq L_{A_0}/N\}$$

where A_0 is the line that is attacked. Since all lines have equal free space S, this gives

$$|proj(A_0)| = N\mathbf{1}\left[S \leq L_{A_0}/N\right]$$

showing that there can be no cascades in this case; after an attack either all lines fail simultaneously or no single line other than those directly attacked fails. It is clear that $|proj(A_0)|$ is monotone increasing in the load L_{A_0} of A_0 so that it is maximized by attacking the line with the maximum load. Repeating this argument recursively, we see that the max-L greedy strategy is optimal for the ER-k-Same-Space problem.

4.7.3 A proof of Theorem 3

The key observation about the ER-k-($C \propto L$) Problem is that, given $C_i = (1+\alpha)L_i$, the load, capacity, and free spaces of lines all follow the same order. Namely, the lines with the largest loads, who shall intuitively be attacked to shed more load on others, are also the ones with the largest free spaces, who are also good to attack given the difficulty of failing them by load redistribution. This eliminates the trade-off faced in the optimal attack problem and simplifies it greatly.

In this setting, the problem does not repeat itself since after load redistribution, it may no longer be the case that all lines have the same tolerance factor (i.e., S/L). However, the aforementioned key property will be maintained throughout. For instance, assume without loss of generality that initial loads are ordered as $L_1 \leq L_2 \leq \cdots \leq L_N$. Then, at any stage of the cascading failures, L_i, C_i, and S_i will all be in increasing order for all $i = 1, 2, \ldots, N$ that are still alive.

With these in mind, we can show the optimality of max-L, C, S-Greedy Algorithms for single line attacks in any system whose loads $L_1, L_2, \ldots, L_N$ and free spaces $S_1, \ldots, S_N$ follow the same order. Since this property will be preserved throughout the cascades and the sequence of attacks doesn't affect the final state of the system, the proof of Theorem 3 will be completed. The rest of the proof is similar to that of Theorem 1 and omitted here for brevity.

4.8 Chapter summary

In this chapter, we continue to understand cascading failures in load-carrying networks under a flow-redistribution based model. Different from last chapter, we focus on assessing the vulnerability of such systems against adversarial attacks. Specifically, we take an attacker's perspective that seeks to fail as many lines as possible by attacking a given number of lines. In particular, in a system with N lines with initial loads $L_1, \ldots, L_N$ and capacities $C_1, \ldots, C_N$, we study the constrained optimization problem of finding k initial lines to be attacked to minimize the final number of alive lines in the system. We give optimal greedy algorithms in several special cases, and prove that a variation of the problem (with a bound on the total load of the initial attack set) is NP-Hard. Several heuristics are developed and their performance is compared with benchmark attacks under various settings. Overall, it is seen that the system is most vulnerable against attacks that target lines with maximum load free-space product $L * (C - L)$. Till now, we provide a comprehensive of the flow-carrying networks under both random and targeted attack. From next chapter, we will look into cascading failures in different interdependent systems and analyze how coupling affect the robustness of the whole system when cascading failure happens.

Part III

Robustness of Interdependent Networks

Chapter 5

Interdependent Flow-carrying Networks under Random Attacks

5.1 Motivation

Recently, researchers have become increasingly aware of the fact that most systems do not live in isolation, and that they exhibit significant *inter-dependencies* with each other. In particular, it has been shown that interdependence and coupling among networks lead to dramatic changes in network dynamics, with studies focusing on cascading failure and robustness [9,69,72,94–97], information and influence propagation [98–102], percolation [11,103–106], etc. One of the most widely studied network dynamics is the cascade (or, spread) of failures. Due to the coupling between diverse infrastructures such as water supply, transportation, fuel and power stations, interdependent networks are tend to be extremely vulnerable [107], because the failure of a small fraction of nodes from one network can produce an iterative cascade of failures in several interdependent networks.

Robustness of interdependent networks has been an active research field after the seminal paper of Buldyrev et al. [9], with the key result being interdependent networks are more vulnerable than their isolated counterparts. However, existing works on cascading failures in interdependent networks focus extensively on percolation-based models [9, 11–15], where a node can function only if it belongs to the largest connected (i.e., giant) component of its own network. While such models are suitable for communication networks, they fail to accurately

capture the dynamics of cascading failures in many real-world systems that are tasked with transporting physical commodities; e.g., power networks, traffic networks, etc. In such flow networks, failure of nodes (or, lines) lead to *redistribution* of their load to functional nodes, potentially *overloading* and failing them. As a result, the dynamics of failures is governed primarily by load redistribution rather than the structural changes in the network. A real-world example to this phenomenon took place on July 21, 2012, when a heavy rain shut down a metro line and caused 100 bus routes to detour, dump stop, or stop operation completely in Beijing [16].

In this chapter, we initiate a study on robustness of interdependent networks under a load redistribution based cascading failure model. Our approach is inspired by the fiber-bundle model that has been extensively used to investigate the fracture and breakdown of a broad class of disordered systems; e.g., magnets driven by an applied field [108], earthquakes [109,110], power system failure [111], social phenomena [112]. This model has already been demonstrated to exhibit *rich* transition behavior in a single network setting under random attacks of varying size, while being able to capture some key characteristics of real-world cascades [80,111]. In our case, the equal and global redistribution rule from the fiber-bundle model enables us to focus on how coupling and interdependence of two arbitrary networks affect their overall robustness, even if individual network topologies might be unknown.

We extend the fiber-bundle-like cascading failure model to interdependent networks as follows. Assume that the system consists of n *coupled* networks each with a given number of transmission *lines*. Every line is given an initial load L and a capacity C defined as the maximum load it can tolerate; if the load on the line exceeds its capacity (for any reason) the line is assumed to fail. The main ingredient of the model is the load redistribution rule: upon failure of a line in any network, the load it was carrying before the failure will be redistributed among all networks in the system, with the proportion received by each network being determined by the *coupling coefficients* across networks; see Section 5.2 for precise details. Within each network, we adopt the fiber-bundle-like model [80, 111] and distribute this received load

equally among all *functional* lines. With appropriate meanings of load and capacity, this type of load oriented models can capture the dependencies in a wide range of physical systems; e.g., two smart-grid operators coupled to provide better service [8], two banks highly correlated for collective risk shifting [113], or two interacting transportation networks [13].

Another way to view the model is to treat the component networks as small communities or regions that compose a bigger network. In this newly formed network, flow is not redistributed equally upon failure, but the fraction of load a node will receive from the failed node is based on the region or community it belongs. The coupling coefficients that we mentioned above can be viewed as the redistribution factor inside each community or region. For the ease of analyzing and to give a clear picture of how flow is redistributed among different component networks, we will continue with interdependent network structure; while we note that one can merge the component networks in an interdependent flow-carrying system into a single network, where the redistribution rule is heterogeneous and more general.

5.2 Model definition

We consider a system composed of n networks that interact with each other. Let $\mathcal{N} = \{1, \ldots, n\}$ denote the set of all networks in the system. For each $i \in \mathcal{N}$, we assume that network i has N_i lines $\mathcal{L}_{1,i}, \ldots, \mathcal{L}_{N_i,i}$ with initial loads $L_{1,i}, \ldots, L_{N_i,i}$. Each of these lines is associated with a capacity $C_{1,i}, \ldots, C_{N_i,i}$ above which the line will be tripped. In other words, $C_{k,i}$ defines the maximum flow that line k in network i can sustain and is given by

$$C_{k,i} = L_{k,i} + S_{k,i}, \qquad i \in \mathcal{N}, \quad k = 1, \ldots, N_i$$

where $S_{k,i}$ denotes the free space on line k in network i, i.e., the maximum amount of extra load it can take. The load-free space pairs $\{L_{k,i}, S_{k,i}\}_{k=1}^{N_i}$ are independently and identically distributed with

$$P_{L_i S_i}(x, y) := \mathbb{P}\left[L_{k,i} \leq x,\ S_{k,i} \leq y\right], \quad k = 1, \ldots, N_i$$

for each $i \in \mathcal{N}$. The corresponding joint probability density function is given by $p_{L_iS_i}(x,y) = \frac{\partial^2}{\partial x \partial y} P_{L_iS_i}(x,y)$. In order to avoid trivial cases, we assume that $S_{k,i} > 0$ and $L_{k,i} > 0$ with probability one for each $i \in \mathcal{N}$ and each $k = 1, \ldots, N_i$. Finally, we assume that the marginal densities $p_{L_i}(x)$ and $p_{S_i}(y)$ are continuous on their support.

Initially, $1 - p_i$ fraction of lines are attacked (or failed) randomly in network i, where $p_i \in [0,1]$. The load on failed lines will be redistributed within the original network and/or shed to other coupled networks depending on the underlying redistribution rules governing the system. Further failures may then take place within the initially attacked network or in the coupled ones due to lines undertaking extra load exceeding their capacity; this in turn leads to further redistribution in all constituent network, potentially leading to a *cascade* of failures. The cascade of failures taking place simultaneously within and across networks leads to an interesting dynamical behavior and an intricate relationship between the level of coupling and the system's overall robustness.

One of our main goals in this paper is to characterize the fraction of alive lines in each network at that 'steady state'; i.e., at the point where cascades stop. To that end, we provide a *mean-field* analysis of dynamical process of cascading failures. Under this approach, it is assumed that when a line fails, its flow will be redistributed to its own network as well as to other networks with the proportion redistributed to each network determined by *coupling coefficients* among the networks. The proportion of load to be shed from a failed line in network i to network j is determined by the coupling coefficient a_{ij}, where we have $\sum_{j \in \mathcal{N}} a_{ij} = 1$ for all i in $\mathcal{N}$; thus, $1 - \sum_{j \in \mathcal{N} - \{i\}} a_{ij}$ gives the fraction of the load that will be redistributed internally in network i.. Each network will then distribute its own share of the failed load *equally and globally* among all of its remaining lines.

For the ease of exposition, we consider a two-network system in the rest of the paper, although our results can be extended trivially to arbitrary number of networks. Consider a system composed of networks A and B that are *interdependent* in the following manner [1]: when

[1]Of course, there are other ways for two networks to be "interdependent" with each other. Here, we use this term with its general meaning, i.e., that failures in one network may lead to failures in the other and vice

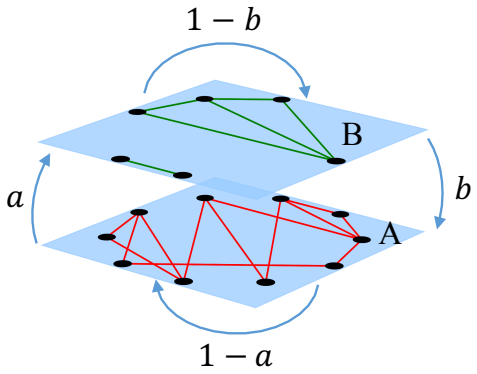


Figure 5.1: *Illustration of a two-network system. When failures happen in network B, b-portion of the failed loads goes to network A and $(1-b)$-portion stays in B. Similarly in network A, $(1-a)$-portion stays and a-portion goes to B. Failed loads will be redistributed equally and globally among the remaining lines in each network.*

a failure happens in network A, a fraction of the failed load is transferred to network B, while the remaining $1-a$ fraction being redistributed internally in A. Similarly upon failures in network B, b fraction of the failed load will be shed to network A; here $a, b \in [0,1]$ are system defined constants. An illustration of the system can be found in Figure 5.1. We assume that initially $1-p_1$ fraction of lines in network A and $1-p_2$ fraction of lines in network B fail randomly. The initial attacks may cause cascading failures, and if one of the network collapses (i.e., if all of its lines fail) during this process, the other network will take over the rest of the load in it and function as a single network from that point on. Throughout, we let $n_{\infty,A}(p_1)$ and $n_{\infty,B}(p_2)$ denote the expected *final* fraction of alive lines of network A and network B when $1-p_1$ and $1-p_2$ fraction of lines is randomly attacked in each network:

$$n_{\infty,A}(p_1) := \lim_{N_A \to \infty} \frac{\mathbb{E}\left[|\mathcal{N}_{\text{surviving A}}(p_1)|\right]}{N_A} \tag{5.1}$$

$$n_{\infty,B}(p_2) := \lim_{N_B \to \infty} \frac{\mathbb{E}\left[|\mathcal{N}_{\text{surviving B}}(p_2)|\right]}{N_B} \tag{5.2}$$

where $\mathcal{N}_{\text{surviving A}} \subset \{1, \ldots, N_A\}$ is the set of lines that are still functioning at the steady state of network A, similarly for $\mathcal{N}_{\text{surviving B}}$. The *robustness* of the system will be evaluated by the

versa, potentially leading to a cascade of failures. Our model constitutes a special case where interdependence emerges from the *inter-connectivity* between the two networks

behavior $n_{\infty,A}(p_1)$ and $n_{\infty,B}(p_2)$ for all attack sizes.

5.3 Analytical results

We now provide the mean-field analysis of cascading failures in the two-network interdependent system. Without loss of generality, we assume that both networks have the same number of lines, i.e., $N_A = N_B = N$. We assume that time is divided into discrete steps, $t = 1, 2, \ldots$. For each time stage t, and with $X \in \{A, B\}$, we use the following notation:

$f_{t,X}$: fraction of failed lines until t;

$F_{t,X}$: total load from lines that fail exactly at time t within network X;

$Q_{t,X}$: extra load to be redistribution at t per alive line in X;

$N_{t,X}$: number of alive lines at t in X before redistribution.

In what follows, we occasionally provide expressions only for the quantities regarding network A, while the corresponding expressions for network B (that are omitted in the text for brevity) can be obtained similarly.

Initially, $1 - p_1$ fraction of lines in network A and $1 - p_2$ fraction of lines in network B are attacked (or failed) randomly. Thus, the fraction of failed lines within each network at $t = 0$ is given by

$$f_{0,A} = 1 - p_1, \quad f_{0,B} = 1 - p_2$$

, while the number of alive lines satisfy

$$N_{0,A} = (1 - f_{0,A})N = p_1 N$$
$$N_{0,B} = (1 - f_{0,B})N = p_2 N$$

Because the initially attacked lines are selected uniformly at random, the total load from failed

lines (in the mean-field sense) satisfy

$$F_{0,A} = \mathbb{E}\left[L_A\right] \cdot f_{0,A} \cdot N = \mathbb{E}\left[L_A\right] \cdot (1 - p_1) \cdot N$$
$$F_{0,B} = \mathbb{E}\left[L_B\right] \cdot f_{0,B} \cdot N = \mathbb{E}\left[L_B\right] \cdot (1 - p_2) \cdot N$$

Based on the equal redistribution rule and the load shedding rule between the two interdependent networks, the extra load per alive line in network A at $t = 0$ is:

$$\begin{aligned} Q_{0,A} &= \frac{(1-a) \cdot F_{0,A} + b \cdot F_{0,B}}{(1 - f_{0,A})N} \\ &= \frac{(1-a) \cdot \mathbb{E}\left[L_A\right] \cdot (1 - p_1) + b \cdot \mathbb{E}\left[L_B\right] \cdot (1 - p_2)}{p_1} \end{aligned}$$

and similarly for network B:

$$Q_{0,B} = \frac{a \cdot \mathbb{E}\left[L_A\right] \cdot (1 - p_1) + (1-b) \cdot \mathbb{E}\left[L_B\right] \cdot (1 - p_2)}{p_2}$$

At stage $t = 1$, line k in network A that survives the initial attack will fail if and only if the updated loads exceed its capacity, i.e., if $L_{k,A} + Q_{0,A} \geq L_{k,A} + S_{k,A}$, or equivalently, if $S_{k,A} \leq Q_{0,A}$. Based on this condition, the fraction of failed lines at $t = 1$ is given by

$$\begin{aligned} f_{1,A} &= f_{0,A} + (1 - f_{0,A}) \cdot \mathbb{P}\left[S_A \leq Q_{0,A}\right] \\ &= 1 - (1 - f_{0,A})\mathbb{P}\left[S_A > Q_{0,A}\right] \end{aligned}$$

To compute the extra load per alive line in each network at $t = 1$, we need to know the lines that fail exactly at this stage in each network (so that their load can be appropriately redistributed to both networks according to the coupling coefficients). Namely, we need to find the lines that survive the initial attack, but have smaller free space than the redistributed load $Q_{0,A}$ or $Q_{0,B}$ from the previous stage. Let $\mathcal{A}$ and $\mathcal{B}$ be the initial set of lines that are attacked

or failed initially in network A and B, respectively. Then, the total load on these failed lines in network A at $t = 1$ can be derived as

$$\begin{aligned} F_{1,A} &= \mathbb{E}\left[\sum_{i\notin\mathcal{A}, S_{i,A}\leq Q_{0,A}} (L_{i,A} + Q_{0,A})\right] \\ &= \mathbb{E}\left[\sum_{i\notin\mathcal{A}} (L_{i,A} + Q_{0,A}) \cdot \mathbf{1}\left[S_{i,A} \leq Q_{0,A}\right]\right] \\ &= p_1 N \mathbb{E}\left[(L_A + Q_{0,A}) \cdot \mathbf{1}\left[S_A \leq Q_{0,A}\right]\right] \end{aligned}$$

where $\mathbf{1}[\cdot]$ is the indicator function [2]; here we used the fact that for each line i in A, L_i, S_i follow the same distribution p_{L_A,S_A}. Similarly for network B, we have

$$\begin{aligned} F_{1,B} &= \mathbb{E}\left[\sum_{i\notin\mathcal{B}, S_{i,B}\leq Q_{0,B}} (L_{i,B} + Q_{0,B})\right] \\ &= p_2 N \mathbb{E}\left[(L_B + Q_{0,B}) \cdot \mathbf{1}\left[S_B \leq Q_{0,B}\right]\right] \end{aligned}$$

The load of these lines failed at stage 1 will then be redistributed internally and across network, based on the aforementioned coupling coefficients. This leads to the extra load per alive line in network A at $t = 1$ being given by

$$\begin{aligned} Q_{1,A} &= Q_{0,A} + \frac{(1-a)\cdot F_{1,A} + b \cdot F_{1,B}}{N(1-f_{1,A})} \\ &= Q_{0,A} + \frac{\begin{array}{r}(1-a)\cdot p_1 \cdot \mathbb{E}\left[(L_A + Q_{0,A})\cdot \mathbf{1}\left[S_A \leq Q_{0,A}\right]\right] \\ + b \cdot p_2 \cdot \mathbb{E}\left[(L_B + Q_{0,B})\cdot \mathbf{1}\left[S_B \leq Q_{0,B}\right]\right]\end{array}}{1 - f_{1,A}} \end{aligned}$$

$Q_{1,B}$ can be written in a similar manner.

At $t = 2$, more lines will fail because of the redistribution in the previous stage. The condition for a line to fail exactly at $t = 2$ is: (i) it doesn't belong to the initial attack set $\{\mathcal{A}$,

[2]Let E be an event. Then, $\mathbf{1}[E]$ is a Binomial random variable that takes the value of 1 if E takes place, and 0 otherwise

$\mathcal{B}\}$; (ii) it survived the redistribution in the previous stage $t = 1$; and (iii) its capacity is less than the updated total load after redistribution at $t = 2$. From this we can derive the fraction of failed lines till $t = 2$ as

$$f_{2,A} = 1 - (1 - f_{1,A})\mathbb{P}\left[S_A > Q_{1,A} \mid S_A > Q_{0,A}\right]$$
$$f_{2,B} = 1 - (1 - f_{1,B})\mathbb{P}\left[S_B > Q_{1,B} \mid S_B > Q_{0,B}\right]$$

Then, the total load from lines that fail exactly at $t = 2$ in network A is given by

$$\begin{aligned} F_{2,A} &= \mathbb{E}\left[\sum_{i\notin\mathcal{A}, Q_{0,A}<S_{i,A}\leq Q_{1,A}} (L_{i,A} + Q_{1,A})\right] \\ &= p_1 N \mathbb{E}\left[(L_A + Q_{1,A})\mathbf{1}\left[Q_{0,A} < S_A \leq Q_{1,A}\right]\right] \end{aligned}$$

Similarly in network B, we have

$$\begin{aligned} F_{2,B} &= \mathbb{E}\left[\sum_{i\notin\mathcal{B}, Q_{0,B}<S_{i,B}\leq Q_{1,B}} (L_{i,B} + Q_{1,B})\right] \\ &= p_2 N \mathbb{E}\left[(L_B + Q_{1,B})\mathbf{1}\left[Q_{0,B} < S_B \leq Q_{1,B}\right]\right] \end{aligned}$$

With the total loads on failed lines $F_{2,A}$, $F_{2,B}$ and the fraction of failed lines $f_{2,A}$, $f_{2,B}$ in each network, the extra load per alive line in network A at stage $t = 2$ can be calculated as

$$\begin{aligned} Q_{2,A} &= Q_{1,A} + \frac{(1-a)F_{2,A} + bF_{2,B}}{N(1 - f_{2,A})} \\ &= Q_{1,A} + \frac{\begin{array}{r}(1-a)\cdot p_1 \cdot \mathbb{E}\left[(L_A + Q_{1,A})\cdot \mathbf{1}\left[Q_{0,A} < S_A \leq Q_{1,A}\right]\right] \\ + b \cdot p_2 \cdot \mathbb{E}\left[(L_B + Q_{1,B})\cdot \mathbf{1}\left[Q_{0,B} < S_B \leq Q_{1,B}\right]\right]\end{array}}{1 - f_{2,A}} \end{aligned}$$

A similar expression gives $Q_{2,B}$.

In light of the above derivation, the form of the recursive equations is now clear: for each

time stage $t = 0, 1, \ldots,$ we have

$$
\begin{aligned}
f_{t+1,A} &= 1 - (1 - f_{t,A})\mathbb{P}\left[S_A > Q_{t,A} \mid S_A > Q_{t-1,A}\right] \\
N_{t+1,A} &= (1 - f_{t+1,A})N \\
Q_{t+1,A} &= Q_{t,A} + \frac{\begin{array}{r}(1-a)\cdot p_1 \cdot \mathbb{E}\left[(L_A + Q_{t,A})\cdot \mathbf{1}\left[Q_{t-1,A} < S_A \le Q_{t,A}\right]\right] \\ + b \cdot p_2 \cdot \mathbb{E}\left[(L_B + Q_{t,B})\cdot \mathbf{1}\left[Q_{t-1,B} < S_B \le Q_{t,B}\right]\right]\end{array}}{1 - f_{t+1,A}},
\end{aligned}
\tag{5.3}
$$

and similarly for network B.

From (5.3) we can see that the cascade of failures will stop and the steady state will be reached only when the number of alive lines doesn't change in both networks, i.e., $N_{t+2,A} = N_{t+1,A}$, $N_{t+2,B} = N_{t+1,B}$. This is equivalent to having

$$
\begin{aligned}
&\mathbb{P}\left[S_A > Q_{t+1,A} \mid S_A > Q_{t,A}\right] = 1, \text{ and} \\
&\mathbb{P}\left[S_B > Q_{t+1,B} \mid S_B > Q_{t,B}\right] = 1
\end{aligned}
\tag{5.4}
$$

In other words, whenever we have finite $Q_{t+1,A}$, $Q_{t,A}$, $Q_{t+1,B}$ and $Q_{t,B}$ values that satisfy (5.4), cascading failures will stop and the system will reach the steady state.

The recursive expressions (5.3) can be simplified further in a way that will make computing the final system sizes (i.e., fraction of alive lines at steady-state) much easier. Firstly, we use the first expression in (5.3) repeatedly for each $t = 0, 1, \ldots$ to get

$$
\begin{aligned}
1 - f_{t+1,A} &= (1 - f_{t,A})\mathbb{P}\left[S_A > Q_{t,A} \mid S_A > Q_{t-1,A}\right] \\
1 - f_{t,A} &= (1 - f_{t-1,A})\mathbb{P}\left[S_A > Q_{t-1,A} \mid S_A > Q_{t-2,A}\right] \\
&\vdots \\
1 - f_{1,A} &= (1 - f_{0,A})\mathbb{P}\left[S_A > Q_{0,A}\right]
\end{aligned}
$$

Multiplying these equations together, we obtain

$$1 - f_{t+1,A} = (1 - f_{0,A}) \prod_{\ell=0}^{t} \mathbb{P}\left[S_A > Q_{\ell,A} \mid S_A > Q_{\ell-1,A}\right],$$

where we set $Q_{-1,A} = 0$ for convenience. Using the fact that $Q_{t,A}$ is non-decreasing in t, i.e., $Q_{t+1,A} \geq Q_{t,A}$ for all t, we then get

$$\begin{aligned} 1 - f_{t+1,A} &= (1 - f_{0,A}) \cdot \frac{\mathbb{P}\left[S_A > Q_{t,A}\right]}{\mathbb{P}\left[S_A > Q_{t-1,A}\right]} \cdots \frac{\mathbb{P}\left[S_A > Q_{1,A}\right]}{\mathbb{P}\left[S_A > Q_{0,A}\right]} \cdot \mathbb{P}\left[S_A > Q_{0,A}\right] \\ &= p_1 \mathbb{P}\left[S_A > Q_{t,A}\right] \end{aligned} \tag{5.5}$$

as we recall that $f_{0,A} = 1 - p_1$.

Using the simplified result (5.5) in (5.3), we now get

$$\begin{aligned} f_{t+1,A} &= 1 - p_1 \mathbb{P}\left[S_A > Q_{t,A}\right] \\ N_{t+1,A} &= p_1 \mathbb{P}\left[S_A > Q_{t,A}\right] N \\ Q_{t+1,A} &= Q_{t,A} + \frac{\begin{array}{r}(1-a) \cdot p_1 \cdot \mathbb{E}\left[(L_A + Q_{t,A}) \cdot \mathbf{1}\left[Q_{t-1,A} < S_A \leq Q_{t,A}\right]\right] \\ + b \cdot p_2 \cdot \mathbb{E}\left[(L_B + Q_{t,B}) \cdot \mathbf{1}\left[Q_{t-1,B} < S_B \leq Q_{t,B}\right]\right]\end{array}}{p_1 \mathbb{P}\left[S_A > Q_{t,A}\right]} \end{aligned} \tag{5.6}$$

leading to a much more intuitive expression than before. To see why (5.6) makes sense realize that for a line to survive stage $t+1$ without failing, it is necessary and sufficient that it survives the initial attack (which happens with probability p_1 for line in network A) *and* its free-space is greater than the total additional load $Q_{t,A}$ that has been shed on it (which happens with probability $\mathbb{P}\left[S_A > Q_{t,A}\right]$. This explains the first and second expressions in (5.6). For the last equation that computes $Q_{t+1,A}$, the extra load per alive line at the end of stage $t+1$ (to be redistributed at stage $t+2$), we write it as the previous extra load $Q_{t,A}$ plus the extra load from lines that fail *precisely* at stage $t+1$. For a line in network A, failing precisely at stage

$t+1$ implies that the line was not in the initial attack (happens with probability p_1) *and* its free space falls in $(Q_{t-1,A}, Q_{t,A}]$ so that it survived the previous load shedding stage but not the current one. Arguing similarly for lines in network B and recalling the redistribution rule based on coupling coefficients, we can see that the nominator in the second term of $Q_{t+1,A}$ (in (5.6)) gives the additional new load that will be shed on the alive lines of A. The whole expression is now understood upon recalling that $p_1\mathbb{P}\left[S_A > Q_{t,A}\right]$ gives the fraction of lines from A that survive stage $t+1$ to take this extra load.

It is now easy to realize that the dynamics of cascading failures is fully governed and understood by the recursions on $Q_{t,A}, Q_{t,B}$ given by

$$Q_{t+1,A} = Q_{t,A} + \frac{\begin{array}{c}(1-a)\cdot p_1 \cdot \mathbb{E}\left[(L_A + Q_{t,A})\cdot \mathbf{1}\left[Q_{t-1,A} < S_A \leq Q_{t,A}\right]\right] \\ + b\cdot p_2 \cdot \mathbb{E}\left[(L_B + Q_{t,B})\cdot \mathbf{1}\left[Q_{t-1,B} < S_B \leq Q_{t,B}\right]\right]\end{array}}{p_1\mathbb{P}\left[S_A > Q_{t,A}\right]} \tag{5.7}$$

$$Q_{t+1,B} = Q_{t,B} + \frac{\begin{array}{c}a\cdot p_1 \cdot \mathbb{E}\left[(L_A + Q_{t,A})\cdot \mathbf{1}\left[Q_{t-1,A} < S_A \leq Q_{t,A}\right]\right] \\ + (1-b)\cdot p_2 \cdot \mathbb{E}\left[(L_B + Q_{t,B})\cdot \mathbf{1}\left[Q_{t-1,B} < S_B \leq Q_{t,B}\right]\right]\end{array}}{p_2\mathbb{P}\left[S_B > Q_{t,B}\right]} \tag{5.8}$$

with the conditions for reaching the steady-state still being (5.4). Put differently, in order to find the *final* system sizes, we need to iterate (5.7)-(5.8) for each $t = 0, 1, \ldots$ until the stop condition (5.4) is satisfied. Let $t^\star$ be the stage steady-state is reached and $Q_A^\star, Q_B^\star$ be the corresponding values at that point. The final system sizes $n_{\infty,A}$ and $n_{\infty,B}$, defined as the expected fraction of alive lines in network A and B at the steady state, respectively, can then be computed simply from (viz. (5.5))

$$\begin{aligned} n_{\infty,A} &= 1 - f_{\infty,A} = p_1\mathbb{P}\left[S_A > Q_A^\star\right] \\ n_{\infty,B} &= 1 - f_{\infty,B} = p_2\mathbb{P}\left[S_B > Q_B^\star\right]. \end{aligned} \tag{5.9}$$

The expressions given above for the steady-state of cascading failures in interdependent systems constitute a non-deterministic, nonlinear system of equations, which often do not have to closed-form solution; contrast this with the single network [111] case, where it is possible

to provide a closed form solution to the final system size. Therefore, in the interdependent network case, we solve $\{Q_A^\star,\ Q_B^\star\}$ by numerically iterating over (5.7)-(5.8). The difficulty of obtaining a closed-form expression for final system sizes arises due to the recursive shedding of load across the two networks. At each stage of the cascade, both networks send a portion of the load from its failed lines to the other network, while receiving a portion of load from the lines failed in the coupled network. Furthermore, the load a line was carrying right before failure depends directly on the extra load per alive line (which decide who fails in the next stage) at the time of its failure. This is why we need to keep track of the set of lines that fail *precisely* at a particular stage to be able to obtain an exact account of these loads [3]. As a result, the final system size can only be obtained by running over the iterations and identifying the first stage at which the stop conditions (5.4) are satisfied.

5.4 Numerical results

5.4.1 Final system size under different system parameters

To verify our analysis with simulations, we choose different load-free space distributions under various coupling coefficients. Throughout, we consider three commonly used families of distributions: i) Uniform, ii) Pareto, and iii) Weibull. These distributions are chosen here because they cover a wide range of commonly used and representative cases. In particular, uniform distribution provides an intuitive baseline. Distributions belonging to the Pareto family are also known as a *power-law* distributions and have been observed in many real-world networks including the Internet, the citation network, as well as power systems [79]. Weibull distribution is widely used in engineering problems involving reliability and survival analysis, and contains several classical distributions as special cases; e.g., Exponential, Rayleigh, and Dirac-delta.

In all simulations, we fix the network size at $N = 10^7$, and for each set of parameters being considered we run 20 independent experiments. The results are shown in Fig. 5.2 where

[3]This is also evident from (5.3) where we see that Q_{t+1} depends not only on Q_t but also on Q_{t-1}

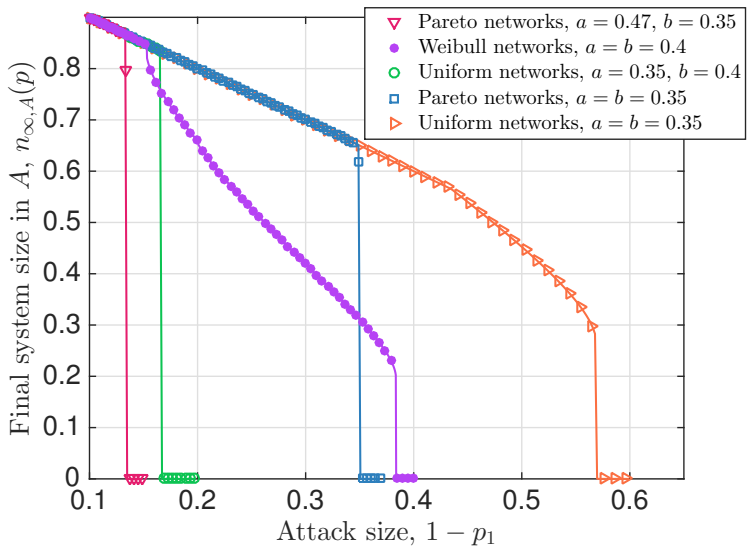


Figure 5.2: *Final system size under different load-free space distributions and coupling coefficients. We observe interesting transition behaviors under different load-free space distributions and coupling level, and the simulation represented in symbol matches with the analytical results represented in lines.*

symbols represent the empirical value of the final system size $n_{\infty,A}$ of network A (obtained by averaging over 20 independent runs for each data point), and lines represent the analytical results computed from (5.9). We see that theoretical results match the simulations very well in all cases.

The plots in Fig. 5.2 demonstrate the effect of the load-free space distribution as well as coupling level on the robustness of the resulting interdependent system. We see that both the family that the distribution belongs to (e.g., Uniform, Weibull, or Pareto) as well as the specific parameters of the family affect the behavior of $n_{\infty,A}(p)$. For instance, the curves representing the two cases where load and free space in both networks follow a Uniform distribution demonstrate that both abrupt ruptures and ruptures with a preceding divergence are possible in this setting, depending on the parameters. Both cases on Pareto networks give an abrupt breakdown at the final point, and we see that Weibull distribution gives rise to a richer set of possibilities for the transition of final system size $n_{\infty,A}(p)$. Namely, we see that not only we can observe an abrupt rupture, or a rupture with preceding divergence (i.e., a second-order transition followed by a first-order breakdown), it is also possible that $n_{\infty,A}(p)$ goes through a

first-order transition (that does not breakdown the system) followed by a second-order transition that is followed by an ultimate first-order breakdown; see the behavior of the purple circled line in Fig. 5.2. Thus in the next section, we will use Weibull distribution to explore the interesting transition behaviors observed in interdependent systems composed of two identical networks.

5.4.2 Transition behavior for two identical networks

To explore the effect of coupling and interdependency on the robustness of networks, we couple two (statistically) identical networks. Put differently, we consider networks A and B where the load and capacity of each of their lines are drawn independently from the same distribution. We also assume that they are coupled together in a symmetric way, i.e., that $a = b$. This is a commonly seen case of an interdependent systems where networks of similar characteristics establish a coupling for mutual benefit; e.g., two grid distributors or financial institutions with similar characteristics. More importantly, this will help us understand the affect of coupling with another identical system on the robustness of a given system; the seminal results of Buldyrev et al. [9] suggest that coupling leads to increased vulnerability under percolation based models.

With these motivations in mind, we let the initial loads in both networks follow a Weibull distribution, with shape parameter $k_w = 0.4$, scale parameter $\lambda = 100$, and minimum initial load $L_{min} = 10$. The free space is assigned proportional to the initial load on each line with a tolerance factor α, i.e. $S = \alpha L$ where $\alpha = 0.6$. The network size is fixed at $N = 10^8$. We attack $1 - p$ fraction of lines randomly in network A, and observe the dynamics of failures driven by the load redistribution across and within the two networks. We then compute the final (i.e., steady-state) size of network A as a function of initial attack sizes $1 - p$ under different values of the coupling coefficient a. The results are depicted in Fig. 5.3, where symbols represent simulation results averaged over 20 independent runs, while lines correspond to our analytical results; in all parameter settings, we observed little to no variance in the final system size

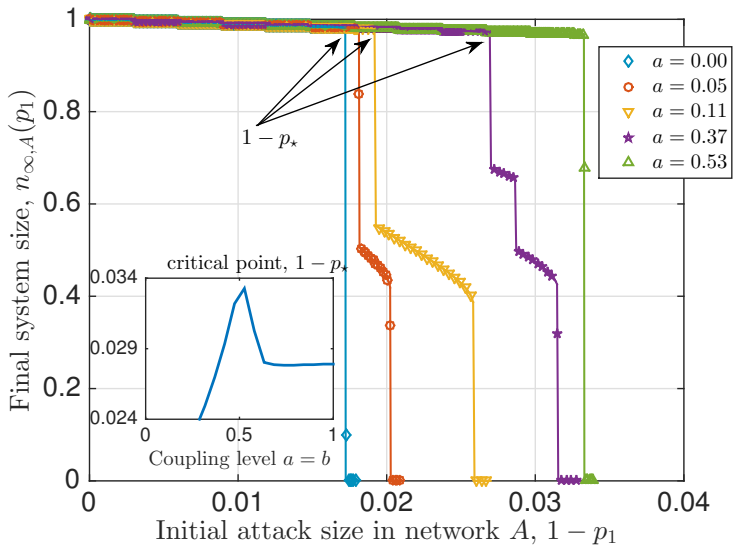


Figure 5.3: *Effect of coupling on the robustness of a single system. We see that contrary to percolation-based models, robustness can indeed be improved by having non-zero coupling between the constituent networks.* Inset. *The critical point* $1 - p_\star$ *defined as the smallest* $1 - p_1$ *at which* $n_{\infty,A}(p_1)$ *deviates from* p_1. *The optimal (i.e., largest)* $1 - p_\star$ *is attained at a non-trivial coupling level* $a = b = \simeq 0.53$.

across the 20 independent experiments [4].

A number of interesting observations can be made from Fig. 5.3. First, we see that coupling level can lead to significant changes in the robustness against random attacks. In particular, the inset in Fig. 5.3 plots the critical attack size $1 - p_\star$ at which the final network size deviates from the p line; given attack size $1 - p$, the final system size can be at most p, which happens when the initial attack does *not* lead to any further failures. The network can be deemed to be more robust when $1 - p_\star$ is larger. *An interesting observation is that unlike the traditional percolation-based models, here coupling with another network might lead to a network to become more robust against failures.* To the best of our knowledge, the only other model where coupling can improve robustness is studied by Brummitt et al. [72], which constitutes an extension of the sandpile model. Perhaps more interestingly, we also see that the optimal robustness (i.e., largest $p_\star$) is attained at a non-trivial coupling level $a = \simeq 0.53$. This suggests that coupling has

[4] We believe this is because the network size N is taken to be very large in the experiments and the random variable $n_{\infty,A}(p_1)$ converges *almost surely* to its mean (e.g., by virtue of Strong Law of Large Numbers); though it is beyond the scope of this paper to prove this.

a multi-faceted impact on robustness and that systems are most robust when they are coupled in a specific, non-trivial way; in Section 5.4.3 we provide some concrete ways to identify such optimum coupling levels.

In addition to affecting the system robustness in non-trivial ways, we see from Figure 5.3 that changing the coupling level can also give rise to different (and, sometimes very interesting) transition behaviors. In particular, we see that network A can go through any one of the transitions demonstrated in previous work [80, 111] for single networks depending on its coupling level with network B. More interestingly, when coupled to network B at a specific level, i.e., with $a = b = 0.37$, it is seen to go through a type of transitions that was not seen in the case when it operates as an isolated network. *This behavior can be described as a sequence of first, second, first, second, and first order transitions, and to the best of our knowledge was not seen before in any model* [5]. In this case, the network stabilizes twice after a sudden drop in the network size during the cascading process, before going through an abrupt final breakdown.

To further explore the transition behavior during the cascading failure process, we plot the number of iterations (i.e., the number of load redistribution steps) needed for the system to reach steady-state. The divergence of the number of iterations is considered to be a good indicator of the onset of large failures, and often suggested as a marker of transition points in simulations; e.g., see [112, 114]. We see that this is indeed the case for our model as well. In Fig. 5.4, we plot the final system size together with the number of iterations taken to reach that final size. The solid lines represent final system size under different coupling coefficients, and the symbols represent the number of iterations needed (divided by the maximum iterations number, 1000) in each case. We see that the number of iterations needed is piece-wise stable with discontinuous jumps corresponding to the transition points, and it diverges near the final breakdown of the network. In Section 5.5, we provide a more detailed discussion on the

[5] We note that the behavior demonstrated here is fundamentally different from the few other cases in the literature where multiple transitions have been reported; e.g., see [97, 106]. There, the type or the number of transitions do not change with the level of coupling across the networks. Instead, multiple transitions arise only when networks with *different* robustness levels are coupled together, and their total (or, average) size is plotted against the size of the attack that is applied to *all* networks involved.

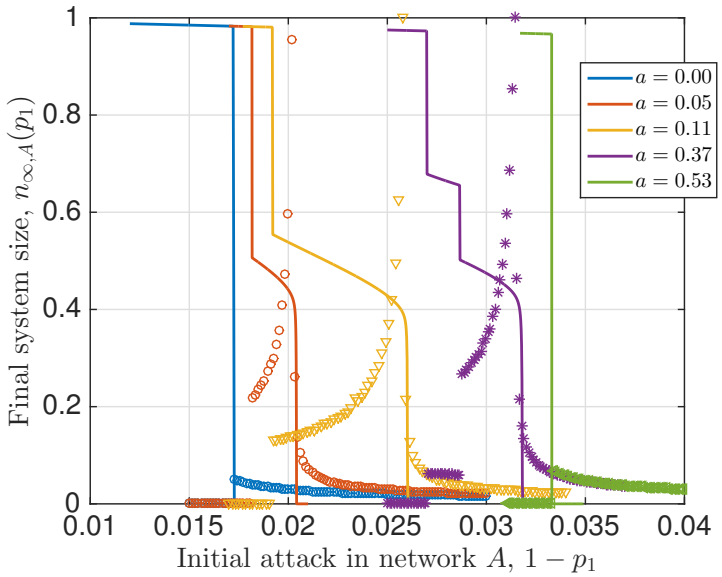


Figure 5.4: *Number of steps needed to reach steady state for identical networks ($a = b$), for various a values. For the case when $a = 0.37$, we observe a novel, unforeseen transition behavior.*

possible correlations between the type and number of transitions a network exhibits with the distribution of its load and free-space.

For a clearer explanation, let us focus on the case when $a = 0.37$ (purple asterisks). We see that both discontinuous drops in the final system size coincide with a discontinuous increase in the number of iterations. As the attack size $1-p_1$ increases further from that second jump, we see a continuous increase in the number of iterations coinciding with the continuous decrease in final system size. This eventually leads to the number of iterations diverging, and as would be expected coincides with the system breaking down entirely.

In Fig. 5.5, the final system size of network A and B are depicted together (for the case $a = 0.37$), showing clearly the effect of interdependence on transition behaviors. Up until $1-p_1 = 0.0287$, there are no failed lines in network B although network A already experiences cascading failures; this indicates that all lines in B are able take the extra load from network A even though A loses a significant fraction of its lines at $1-p_1 = 0.0271$. When some lines start failing in network B at $1-p_1 = 0.0287$, a *large* cascade of failures take place causing a significant number of lines fail from both networks marked by discontinuous drop in the final

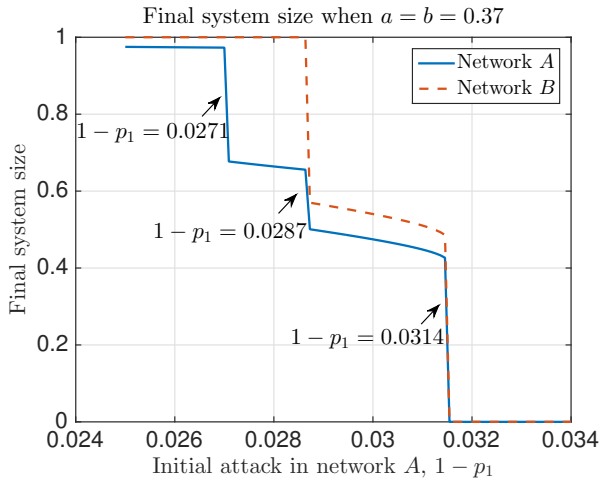


Figure 5.5: *Final system size in two networks when only network A has been attacked initially. The two networks are statistically identical with* $a = b = 0.36$*. Their loads follow a Weibull distribution with* $k_w = 0.4$*,* $\lambda = 100$*,* $L_{min} = 10$*, and* $S = 0.6L$

size of both networks. After this point, the remaining system is able to sustain higher initial attacks (because the lines that survive until this point tend to have *larger* free-space than average). However, when we reach $1 - p_1 = 0.0314$, another large cascade takes place that collapses both networks. This final breakdown is observed almost simultaneously in networks A and B, primarily because once a network collapses, the other network will need to take over all the load in the system, and in most cases will not be able survive on its own.

5.4.3 Optimizing the robustness of an interdependent system

We now discuss how the robustness of an entire interdependent system can be quantified, with an eye towards identifying *optimal* coupling levels that maximize system robustness. Assume that initially $1 - p_1$ fraction of lines from A and $1 - p_2$ fraction of lines from B are attacked randomly. The $p_1, p_2 \in [0, 1]$ plane is naturally divided into four *survival regions* [115]. where i) S_{12} represents the initial attack pair $(1 - p_1, 1 - p_2)$ under which both networks survive, i.e., have *positive* fraction of functional lines when steady state is reached; ii) S_1 represents the case where only network A survives; iii) S_2 represents the case where only network B survives; and iv) S_0 represents the region where no network survives, i.e., the entire system fails with no

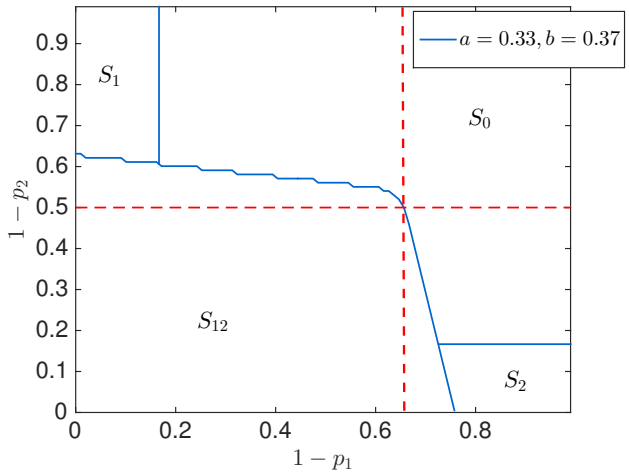


Figure 5.6: *Survival regions of the coupled system under load-redistribution based model. When coupling is introduced, regions where both networks survive or collapse (S_{12} and S_0, respectively) get larger, while regions where only one network survives (S_1 and S_2) shrink significantly.*

alive lines. It is then tempting to study the affect of network coupling on these four regions.

To provide a concrete example, let network A have $L_A \sim U[10, 30]$, $S_A \sim U[40, 100]$, and network B have $L_B \sim U[20, 40]$, $S_B \sim U[30, 85]$, with U denoting *uniform* distribution. The initial load distribution and free space distribution are assumed to be independent in each network. We see from Fig. 5.6 that when there is no coupling ($a = b = 0$), both networks operate in isolation and the survival of A and B are independent from each other; as we would expect, the two dashed lines (in red color) mark the critical attack sizes for A and B when they are in isolation [111]. When we introduce coupling to the system, e.g., with $a = 0.33$ and $b = 0.37$, we see an interesting phenomenon indicating a multi-faceted impact of coupling on system robustness. The region S_{12} where both networks survives enlarges, while S_1, S_2 where only one network survives shrink dramatically. Meanwhile, S_0 where both networks collapse also enlarges. In a nutshell, when coupled together, the two networks are able to help each other to survive larger attack sizes as compared to the case when they are isolated; however, this comes at the expense of also failing together at smaller attack sizes than before.

To further quantify the effect of coupling on system robustness, we consider the setting above while varying the coupling coefficients a and b. For both networks, we deploy the same

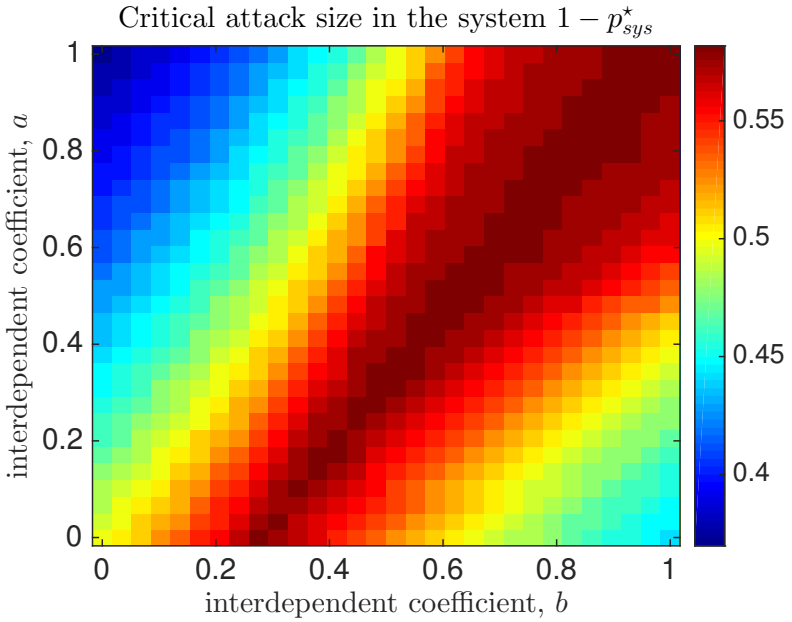
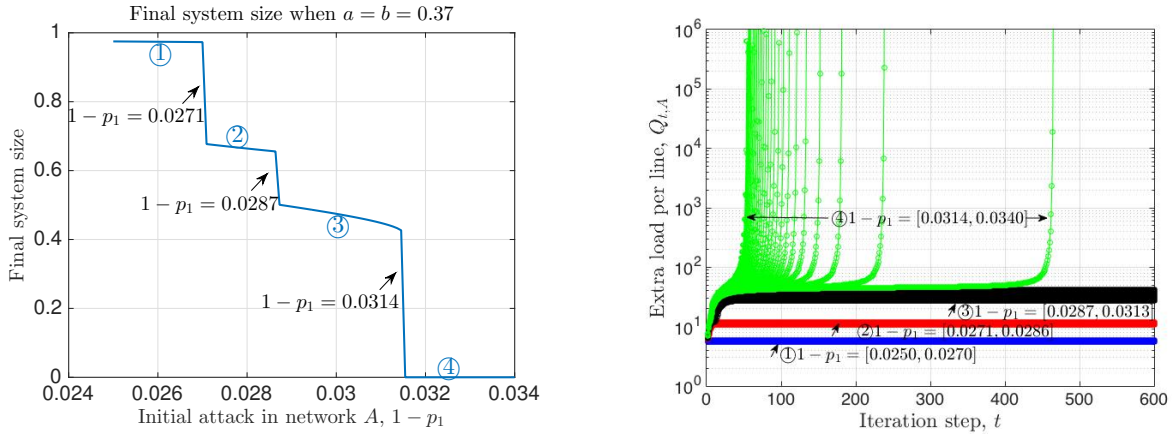


Figure 5.7: *Color map of the critical attack size under different coupling coefficients a and b. Darker colors indicate larger $1-p^{\star}_{sys}$ values, meaning that the interdependent system is more robust.*

initial attack, i.e., $1-p_1 = 1-p_2 = 1-p$, and define the critical system attack size $1-p^{\star}_{sys}$ as the minimum $1-p$ that collapses at least one network in the system when cascading failures stop; i.e., $1-p^{\star}_{sys}$ marks the intersection of the $p_1 = p_2$ line and the boundary of the S_{12} region in Figure 5.6.

The metric $1-p^{\star}_{sys}$ proposed here provides a simple and useful way to quantify the robustness of the overall system. For example, aside from being the smallest attack size needed to be launched on both networks to fail at least one of them completely, it gives a good indication of the *area* of the S_{12} region where both networks are functional at steady-state. In Fig. 5.7 we show the value of $1-p^{\star}_{sys}$ for different coupling coefficients (a, b) using a color map; the darker the graph, the larger is the $1-p^{\star}_{sys}$ value. Using this, one can design an interdependent system to have the optimum coupling levels (a, b) so that robustness of the overall system is maximized (in the sense of maximizing $1-p^{\star}_{sys}$). We see that the optimum (a, b) is not unique, but instead contain in a certain *strip* of the $[0, 1]^2$ plane. This indicates that the robustness of the interdependent system can be optimized even under certain application-specific constraints on the coupling levels a and b; e.g., one might need to have $a = b$ for fairness to both networks,



(a) (b)

Figure 5.8: *Extra load per alive line $Q_{t,A}$ is shown (at different attack sizes $1 - p_1$ on Network A) as a function of cascade step $t = 0, 1, \ldots$, for the setting considered in Figure 5.5. The jumps in the transitions divide the final system curve into four regions (marked with circled numbers), which correspond to four clusters in the $Q_{t,A}$ plots (distinguished by four colors).*

or $a + b = 1$ to bound the total load transfer across networks, etc.

5.5 Explanation on multiple continuous/discontinuous transitions

In this Section, we will explore in more details the underlying reasons for a network to undergo multiple continuous/discontinuous transitions under the flow redistribution model studied in this paper. First of all, we note that whether a line survives or fails a particular stage of cascading failure depends on the the extra load per alive line at that iteration, i.e., $Q_{t,A}$ or $Q_{t,B}$. With this in mind, in Figure 5.8b we plot $Q_{t,A}$ as a function of the iteration step t under the setting of Figure 5.5 (i.e., when network A experiences multiple transitions). In all cases, we vary attack size $1 - p_1$ over a range with small increments, so that a single curve in Figure 5.8b represents the change of $Q_{t,A}$ vs. t under a specific attack size $1 - p_1$.

We observe that each $1 - p_1$ value leads to a variation of $Q_{t,A}$ that belongs to one of the four clusters, distinguished by different colors in Figure 5.8b. For example, as $1 - p_1$ increases from 0.0250 to 0.0271, the corresponding $Q_{t,A}$ curves move up smoothly forming the blue cluster.

At $1-p_1 = 0.0272$, $Q_{t,A}$ experiences a jump, but as $1-p_1$ increases further, $Q_{t,A}$ curves move up continuously until $1-p_1 = 0.0287$, forming the red cluster. The jump between the blue and red clusters at $1-p_1 = 0.0271$ coincides with the first jump in the transition in Figure 5.8a. Similarly, at $1-p_1 = 0.0287$ we observe a second jump in $Q_{t,A}$ curves between the red and black clusters, which corresponds to the second jump in Figure 5.8a. When attack size $1-p_1$ further increases, $Q_{t,A}$ curves keep moving up smoothly until $1-p_1 = 0.0314$ after which $Q_{t,A}$ goes to infinity as $t \to \infty$, meaning that network A collapses completely without any alive lines; the corresponding $Q_{t,A}$ curves for $1-p_1 \geq 0.0315$ form the fourth cluster show by dotted green lines. Not surprisingly, $1-p_1 = 0.0314$ corresponds to the final breakdown point observed in Figure 5.8a.

Another way to read these figures is that after the extra load per non-failed line $Q_{t,A}$ (resp. $Q_{t,B}$) reaches a certain value, the network A (resp. B) goes through a sequence of failures after which it either stabilizes with a large fraction of failed lines, or it can not stabilize and goes through a complete breakdown. These *critical* values of $Q_{t,A}, Q_{t,B}$ and their connection to the emergence of multiple transitions can be understood better in the case of a single network. In [111], we have provided a detailed analysis of the global redistribution model in single networks and demonstrated that the critical transition values are determined by the inequality:

$$g(x) := \mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x]) \geq \frac{\mathbb{E}[L]}{p}, \quad x \in (0, \infty) \tag{5.10}$$

With $x^\star$ denoting the smallest solution of (5.10), the final system size is given by

$$n_\infty(p) = p\mathbb{P}\left[S > x^\star\right]. \tag{5.11}$$

Here x represents *candidate values* for the extra load per alive line at the steady-state; i.e., it represents potential solutions to Q_∞. To see this better, we can rewrite the inequality (5.10)

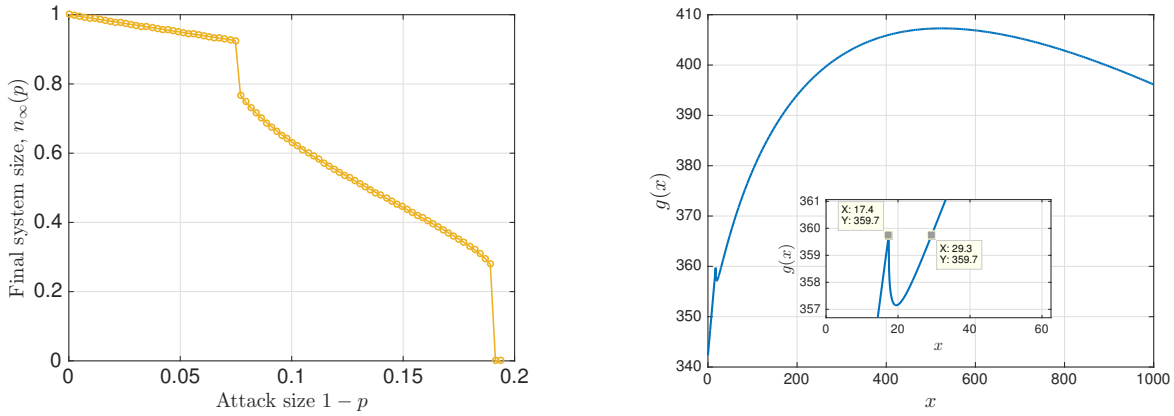
as

$$x \geq \frac{(1-p)\mathbb{E}\left[L\right] + p\mathbb{E}\left[L\mathbf{1}\left[S \leq x\right]\right]}{p\mathbb{P}[S > x]}. \tag{5.12}$$

We can now realize that for any $1-p$ and x for which this inequality holds, the *alternative* attack that kills i) $1-p$-fraction of the lines randomly; and ii) all remaining lines whose free-space is less than x (i.e., that satisfy $S \leq x$), is a *stable* one that does not lead to any single additional line failure. To see this, note that the term $p\mathbb{P}[S > x]$ in (5.12) gives the fraction of lines that survive the alternative attack, where each surviving line having at least x amount of free-space, while $(1-p)\mathbb{E}\left[L\right] + p\mathbb{E}\left[L\mathbf{1}\left[S \leq x\right]\right]$ gives the total load failed initially as a result of the alternative attack. Thus, for a given attack size $1-p$, the smallest x satisfying inequality (5.10) or (5.12) will give us the steady-state extra load per alive line Q_∞.

With these in mind, we now explore the underlying reasons for the final system size $n_\infty(p)$ to exhibit (potentially multiple) discontinuous transitions. From Figure 5.8 and the discussion that follows, we expect discontinuous transitions in $n_\infty(p)$ to appear simultaneously with discontinuous jumps in the behavior of Q_t as $1-p$ varies. We now show that our results given at (5.10)-(5.11) confirm this intuition. To visualize the implications of (5.10)-(5.11) better, we should plot $g(x)$ as a function of x, and find the leftmost intersection of this curve and the horizontal line drawn at $\frac{\mathbb{E}[L]}{p}$. Let this leftmost intersection be denoted by $x^\star(p)$ (with the notation making the dependence of $x^\star$ on the attack size p explicit). The final system size is given from (5.11) as $n_\infty(p) = p\mathbb{P}\left[S > x^\star(p)\right]$. Assuming that the tail of the distribution of S is continuous, we see that $n_\infty(p)$ will exhibit a discontinuous jump if (and only at the points where) $x^\star(p)$, which is analogous to the steady-state extra-load per alive line Q_∞, exhibits a discontinuous jump. This confirms the intuition stated above.

Recall that $x^\star(p)$ is the leftmost intersection of $g(x)$ and $\mathbb{E}\left[L\right]/p$, and assume that $\mathbb{E}\left[L \mid S > x\right]$ is continuous, so that $g(x)$ is continuous. Then, $x^\star(p)$ (and thus the final system size $n_\infty(p)$) *will exhibit one discontinuous jump for every* local *and the global maxima of* $g(x)$. This last statement explains why certain L, S distributions lead only to a single discontinuous jump (since the corresponding $g(x)$ has a single maxima) while others give two (or, potentially



(a) (b)

Figure 5.9: *Multiple transitions in a single network and the corresponding function $g(x)$ (defined at (5.10)) is plotted when L follows Weibull distribution with $k_w = 0.4$, $\lambda = 100$, $L_{min} = 10$, and $S = \alpha L$ where $\alpha = 1.74$. The Inset zooms in to the region where $g(x)$ has a local maximum.*

more) discontinuous transitions. An example for the latter case is given in Figure 5.9. We see that the corresponding function $g(x)$ (Figure 5.9b) exhibits a *local* maxima at $x = 17.4$. As a result, when we search for the leftmost intersection of $g(x)$ and $\mathbb{E}[L]/p$ as p varies from zero to one, we see that at a certain $1-p$ value, the leftmost solution $x^\star(p)$ jumps from $x = 17.4$ to $x = 29.3$, creating a first-order transition in the final system size $n_\infty(p) = p\mathbb{P}[S > x^\star(p)]$. After this point, as attack size $1-p$ increases further, the (leftmost) intersection points increase smoothly, leading to the continuous transition seen in Figure 5.9a, until the global maxima of $g(x)$ is reached. At that $1-p$ value, the leftmost intersection of $g(x)$ and $\mathbb{E}[L]/p$ jumps from a finite value to *infinity* (indicating that there is no x satisfying inequality (5.10)), and the system goes through a discontinuous transition leading to its complete break down.

5.6 Simulation results under global-local combined redistribution model

The main problem considered in this paper, concerning the cascade of failures in two interdependent flow networks, would be expected to depend on the network connectivity patterns

in practical scenarios. However, the approach used in this paper offers physical insight by proposing a *mean field* approach on the setup presented. In fact, the abstraction used in this paper is equivalent *in spirit* to the determination of percolation properties based on degree distributions, mean-field, heterogeneous mean-field, and generating function approaches, etc. In addition, merely topology-based models where the failed load is redistributed solely in the local neighborhood of the failed line (e.g., as in [59, 116, 117]) suffers from two main issues. First of all, it is often not possible to obtain complete analytic results under topology-based redistribution models, even within the single network framework. Thus, unlike the detailed analytical results given in this paper for interdependent networks, one would most likely be constrained to simulation results if a topology-based redistribution model was used. Secondly, models where the failed flow gets redistributed only locally according to a topology cannot capture the *long-range behavior* of failures that are observed in most real-world cascades [115].

With these in mind, we believe our paper exercises a reasonable trade-off of capturing key aspects of real-world cascades while being able to obtain complete analytic results. Nevertheless, we find it useful to complement our analytical results with simulations that demonstrate how network topology affects the robustness properties of interdependent networks. To this end, we consider a model that combines the global redistribution model described in Section 6.2 and the local redistribution model used in [59]. In particular, assume that upon failures in a network, μ fraction of the failed flow is redistributed solely in the local neighborhood of the failed line, while the rest gets redistributed among *all* functional lines. In the case of interdependent networks studied here, we only focus on the intra-topology of networks A and B and still couple them through parameters a and b; i.e., when a line in A fails, a-fraction of the failed flow gets redistributed equally among *all* functional lines of B, while $(1-a)\mu$-fraction gets redistributed locally in A among the neighbors of the failed line, and the remaining $(1-a)(1-\mu)$-fraction gets redistributed among *all* functional lines of A.

With this approach, we recover the model analyzed in our paper when $\mu = 0$, while setting $\mu = 1$ gives a merely topology-based model. We now present a simulation result that shows the

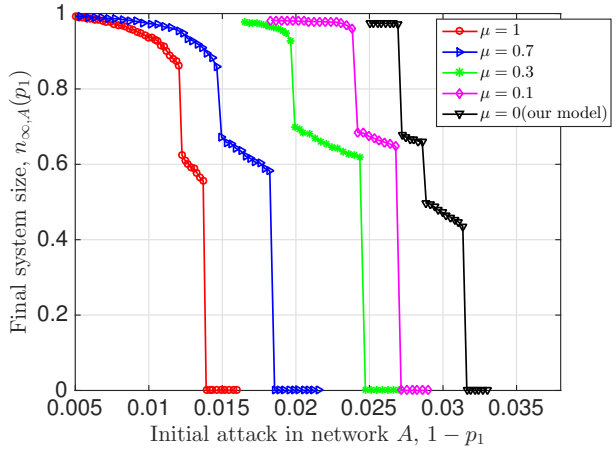


Figure 5.10: *Effect of parameter μ, which controls the fraction of failed load that will be redistributed locally according to network topology, on the robustness of interdependent systems.*

robustness of an interdependent system under different μ values. For convenience, we consider the same set-up used in Fig. 5.5, i.e. the two networks are statistically identical with coupling coefficient $a = b = 0.36$, and their loads follow a Weibull distribution with $k_w = 0.4$, $\lambda = 100$, $L_{\min} = 10$, and $S = 0.6L$. For simplicity, we assume that the topologies of both networks are generated by the Erdős-Rényi model with 9000 nodes and link probability 0.2, leading to a mean number N of links around 8.1×10^6.

The results are depicted in Figure 5.10. As would be expected, as μ decreases from one (purely topology-based model) to zero (the model analyzed in our paper), the robustness of network A increases. In other words, the more fraction of failed flow gets shared globally instead of locally, the more robust the network becomes. This is intuitive since when failed flow is shared globally, the additional load per functional line decreases, leading to a lower chance of triggering cascading failures. Nevertheless, the qualitative behavior of the robustness of network A as the attack size $1-p_1$ increases remains relatively unchanged at different μ values; e.g., in all cases, we observe multiple discontinuous transitions, with continuous transitions in between. This suggests that the mean-field approach used in our analysis (i.e., the case with $(\mu = 0)$) is able to capture very well the *qualitative* behavior of final system size for all μ values.

5.7 Chapter summary

In this chapter, we start to look into interdependent system. To begin with, we studied the robustness of interdependent systems under a flow-redistribution based model. In contrast to percolation-based models that most existing works are based on, our model is suitable for systems carrying a flow (e.g., power systems, road transportation networks), where cascading failures are often triggered by *redistribution* of flows leading to *overloading* of lines. We give a thorough analysis of cascading failures in a system of two interdependent networks initiated by a random attack. We show that (i) the model captures the real-world phenomenon of unexpected large scale cascades: final collapse is always first-order, but it can be preceded by a sequence of several first and second-order transitions; (ii) network robustness tightly depends on the coupling coefficients, and robustness is maximized at non-trivial coupling levels in general; (iii) unlike existing models, interdependence has a multi-faceted impact on system robustness in that interdependency can lead to an improved robustness for each individual network. In the next chapter, we will study the interdependent networks composed of inherently different networks; i.e., cyber-physical systems and the robustness of such systems against cascading failures.

Chapter 6

Robustness of Cyber-Physical Systems

6.1 Introduction and motivation

Today's worldwide network infrastructure consists of a web of interacting cyber-networks (e.g., the Internet) and physical systems (e.g., the power grid). Integrated cyber-physical systems (CPSs) are increasingly becoming the underpinning technology for major industries. The smart grid is an archetypal example of a CPS where the power grid network and the communication network for its operational control are coupled together; the grid depends on the communication network for its control, and the communication network depends on the grid for power. While this coupling with a communication network brings unprecedented improvements and functionality to the power grid, it has been observed [7] that such interdependent systems tend to be fragile against failures, natural hazards, and attacks. For instance, in the event of an attack or random failures in an interdependent system, the failures in one of the networks can cause failures of the dependent nodes in the other network and vice versa. This process may continue in a recursive manner, triggering a cascade of failures that can potentially collapse an entire system. In fact, the cascading effect of even a partial Internet blackout could disrupt major national infrastructure networks involving Internet services, power grids, and financial markets [9]. For example, it was shown [10] that the electrical blackout that affected much of Italy on 28 September 2003 had started with the shutdown of a power station, which led to failures in the Internet communication network, which in turn caused the breakdown of more stations, and so on.

With interdependent systems becoming an integral part of our daily lives, a fundamental question arises as to how we can design an interdependent system in a *robust* manner. Towards this end, a major focus has to be put on understanding their vulnerabilities, and in particular the root cause of the seemingly unexpected but large scale cascading failures. These events are often attributed to a small initial shock getting escalated due to the intricate dependencies within and across the individual (e.g., cyber and physical) counterparts of the system. Therefore, a good understanding of the robustness of many real-worlds systems passes through an accurate characterization and modeling of these inherent dependencies.

Traditional studies in network science fall short in characterizing the robustness of interdependent networks since the focus has mainly been on single networks in isolation; i.e., networks that do not interact with, or depend on any other network. Despite some recent research activity aimed at studying interdependent networks [9,17–21], very few consider engineering aspects of inter-dependent networks and very little is known as to how such systems can be designed to have maximum robustness under certain design constraints; see [22–25] for rare exceptions. The current literature is also lacking interdependent system models that capture fundamental differences between *physical* and *cyber* networks, and enable studying robustness of systems that integrate networks with inherently different behavior. For example, it would be expected that the functionality of the physical subsystem is primarily governed by the physical flows and capacities associated with its components, whereas system-wide connectivity would be the prominent requirement for maintaining functionality in the cyber network. There is thus a need to develop new approaches for modeling and analyzing cascading failures in interdependent cyber-physical systems.

In this chapter, we develop a model that will help understand how failures would propagate in an interdependent system that constitutes physical *and* cyber networks. This requires characterization of *intra*-dependency models for each constituent network as well as an *inter*-dependency model describing the spread of failures *across* networks; see Section 6.2.1 for details. As already mentioned, the main drawback of the current literature on interdependent networks

is that the focus has almost exclusively been on *percolation*-based failure models, where a node can function only if it belongs to the largest connected (i.e., giant) component in the networks. While suitable for cyber or communication networks, such models are not appropriate for networks carrying physical flows; e.g., in power grid, *islanding* is a commonly used strategy for preventing cascades [118].

We provide a thorough analysis of the dynamics of cascading failures in this interdependent system, where failures are initiated by a *random* attack on a certain fraction of nodes. The system robustness, defined as the *steady-state* fraction of nodes that survive the cascade, is characterized in terms of all network parameters involved (e.g., degree distribution of the cyber-network, load-capacity values in the physical-network, network size, attack size, etc.). Analytic results are supported by an extensive numerical study. An interesting finding is that under our model, the system goes through a *complete breakdown* through a *discontinuous* transition with respect to increasing attack size. In other words, the variation of the "mean fraction of functional nodes at the steady state" with respect to "attack size" has a discontinuity at the *critical* attack size above which the system collapses. This indicates that our model's behavior is reminiscent of large but rare blackouts seen in real world, and thus might help explain how small initial shocks can cascade to disrupt large systems that have proven stable with respect to similar disturbances in the past.

We also leverage our main result to investigate how the robustness can be improved by adjusting various parameters defining the interdependent system; e.g., load/capacity values in the physical network and the degree distribution of the cyber-network. This can prove useful in designing an interdependent system so that it has maximum robustness under given constraints. It is important to note that limited prior work revealed unprecedented differences in the behaviors of interdependent networks as compared to single networks. For instance, it has been shown [9, 22] that a network design that is optimal in countering node failures in a single network could be the most catastrophic choice for the resiliency of interdependent networks. For the model considered here, our results reveal an intricate connection between the robustness

of each constituent network when they are isolated and the robustness of the interdependent system formed by them. First of all, when all else is fixed, and the *total* capacity available to all nodes in the physical network is given, the interdependent system becomes more robust when capacities are allocated such that every node has the same *redundant space* (i.e., capacity minus initial load) as compared to the commonly used [59, 77, 84, 85] allocation where nodes are given a redundant space proportional to their initial load. However, the situation becomes much more intricate when the degree distribution of the cyber-network and the redundant space allocation in the physical network are adjusted simultaneously. There, we observe that depending on the degree distribution of the cyber-network, an interdependent system with equal redundant space allocation can be more or less robust than one where redundant space is proportional to load (with mean node degree and initial loads fixed). Also, in contrast with the well-known results in single networks [5] where degree distributions with large variance (e.g., Pareto) are associated with higher robustness (against *random* failures) than cases where the variance is small (e.g., Poisson distribution), we demonstrate that the comparison is more intricate for interdependent systems. In particular, we provide several examples where the interdependent system with a Pareto-distributed cyber-network is more or less robust than one where the cyber-network has Poisson degree distribution, even when all other parameters are kept constant.

We believe this work brings a new perspective to the field of robustness of interdependent networks and might help steer the literature away from the heavily-studied percolation models towards flow-redistribution models, *and* towards models that combine networks with inherently different cascade characteristics (of which CPS is an archetypal example); to the best of our knowledge, this is the first work where the interdependence of two networks with fundamentally different cascade behavior is studied. We believe that our results provide interesting insights on the robustness of interdependent CPSs against random failures and attacks. In particular, despite the simplicity of the models used, our results might capture the *qualitative* behavior of cascades in an interdependent system well. We also believe this work will trigger further

studies (and provide initial ideas) on how node capacities in the physical-network and the topology of the communication network can be designed jointly to maximize the robustness of an interdependent CPS.

6.2 System model

6.2.1 Intra-dependency vs. inter-dependency

Our modeling framework is motivated from the inherent dependencies that exist in many real-world systems including cyber-physical systems. Namely, we characterize how component failures propagate and cascade, both within the cyber or the physical parts of the system (due to "intra-dependency"), as well as across them due to "inter-dependency". The actual meaning of "failure" is expected to be domain-dependent and can vary from a component being physically damaged to a node's inability to carry out its tasks; in all cases we adopt a *binary* model where a node is either fully functional or failed completely and is removed from the system. For ease of exposition, we consider two sub-systems, say A and B.

Assume that network A consists of nodes $\{a_1, \ldots, a_N\}$ and network B consists of nodes $\{b_1, \ldots, b_N\}$. For illustration purposes, we can think of network A as the power network consisting of generators and substations (i.e., the physical network), and network B as the control and communication network consisting of control centers and routers (i.e., the cyber network) – This is a classical example of an interdependent CPS, with the power stations sending data to and receiving control signals from routers, and routers receiving power from substations. Modeling the dependencies within and between networks A and B amounts to answering three questions. First, for both networks we must decide on the set of rules governing how failures would propagate within that network, leading to a characterization of the *intra*-dependencies. For example, we should identify how the failure of a power node a_i affects other substations and generators in the power network A. Similarly, we should identify how the failure of a communication node b_j affects other nodes in B. Finally, we must characterize the

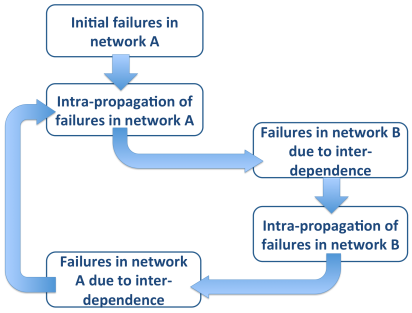


Figure 6.1: *An illustration of failure propagation model in an interdependent system.*

inter-dependence of the two networks, and how interdependence may lead to propagation of failures across them. Namely, we must have a set of rules that specify how the failure of a power station a_i impacts the nodes $\{b_1, \ldots, b_N\}$ in the communication network and vice versa.

Once these modeling questions are answered, the propagation of failures in an interdependent system (consisting of networks A and B) can be studied. Without loss of generality, assume that the failures are initiated in network A due to random failures or attacks. To get a better idea about the role of intra- and inter-dependencies in the cascade of failures, consider an *asynchronous* failure update model, where the effect of intra-dependencies and inter-dependencies are considered in two separate batches, following one another. See Figure 6.1 for an illustration of the asynchronous failure propagation model. The asynchronous failure update assumption eases the implementation and analysis of the model, and can be shown to yield the same steady-state network structures with a synchronous failure update model; just note that failure propagation process is monotone and that (according to our assumption) nodes can not heal once failed.

6.2.2 Proposed model for CPS system

Despite the vast literature on interdependent networks [9, 22, 119, 120], there has been little (if any) attempt to characterize the robustness of interdependent systems where the constituent networks have different intra-dependency behaviors. In the case of CPS, it would be expected that the cyber and physical counterparts obey inherently different rules governing how failures would propagate internally in each network. To this end, we study in this paper an interdepen-

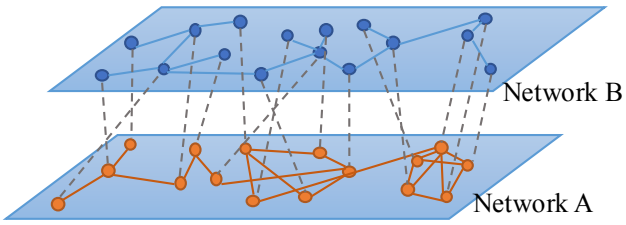


Figure 6.2: *System model illustration for the cyber-physical systems, where network A can be the physical grid, and network B can be the communication network that sends control signals. The interdependence across the two networks are realized through random one-to-one support links shown by dashed lines. Our analysis of cascading failures is based on a* mean-field *approach for network A, meaning that the topology of network A, shown above for illustration purposes, is not taken into account (i.e., assumed to be fully-connected).*

dent system model that consists of two networks with different characteristics governing their *intra*-dependency: i) a *cyber*-network where a node is deemed to be functional as long as it belongs to the largest connected (i.e., giant) component; and ii) a *physical* network where nodes are given an initial *flow* and a *capacity*, and failure of a node results with redistribution of its flow to the remaining nodes, upon which further failures might take place due to *overloading* (i.e., the flow of a node exceeding its capacity). To the best of our knowledge, this is the first work in the literature that studies interdependence between networks with fundamentally different intra-dependency; most existing works are focused on the interdependency between two physical networks (that obey a flow-redistribution-based model) [115], or two cyber-networks (that obey a giant-component-based intra-failure model) [9].

Intra-dependency in Network A. Let network A represent a flow network on nodes $a_1, \ldots, a_N$. Each node a_i is given an initial load (e.g., power flow) $L_1, \ldots, L_N$. The *capacity* C_i of node a_i defines the maximum flow that it can sustain, and is given by

$$C_i = L_i + S_i, \qquad i = 1, \ldots, N, \tag{6.1}$$

where S_i denotes the *free-space* (or, redundancy) available to node a_i. It is assumed that a node *fails* (i.e., outages) if its load exceeds its capacity at any given time. The key assumption of our intra-dependency model for network A is that when a node fails, the load it was carrying

(right before the failure) is redistributed *equally* among all remaining nodes. This leads to an increase in load carried by all remaining nodes, which in turn may lead to further failures of overloaded nodes, and so on, potentially leading to a cascade of failures.

The equal flow redistribution rule takes its roots from the *democratic* fiber bundle model [81,121], and has been recently used by Pahwa et al. [122] in the context of power systems; see also [23,88]. The relevance of the equal flow-redistribution model for power systems stems from its ability to capture the *long-range* nature of the Kirchhoff's law, at least in the *mean-field* sense, as opposed to *topological* models where failed load is redistributed only *locally* among neighboring lines [77,78]; e.g., it was suggested by Pahwa et al. [79] that equal flow redistribution is a reasonable assumption especially under the DC power flow model. In Section 6.5, we confirm via simulations that the mean-field assumption leads to results that are qualitatively very similar to those obtained under different flow-redistribution models based on network topology.

Throughout we assume that the load and free-space pairs (L_i, S_i) are independently and identically distributed with $P_{LS}(x, y) := \mathbb{P}[L \leq x, S \leq y]$ for each $i = 1, \ldots, N$. The corresponding (joint) probability density function is given by $p_{LS}(x, y) = \frac{\partial^2}{\partial x \partial y} P_{LS}(x, y)$. In order to avoid trivial cases, we assume that $S_i > 0$ and $L_i > 0$ with probability one for each a_i. Finally, we assume that the marginal densities $p_L(x)$ and $p_S(y)$ are continuous on their support.

Intra-dependency in Network B. Let network B represent a cyber (e.g., communication) network consisting of nodes $b_1, \ldots, b_N$. In this network, we assume that a node keeps functioning as long as it belongs to the largest (i.e., *giant*) connected component of the network. If a node loses its connection to the giant core of the network, then it is assumed to have failed and can no longer carry out its functions. This percolation-based failure rule, though not suitable for *physical* systems carrying a flow, can be regarded as a reasonable model for *cyber*-networks (e.g., sensor networks) where connectivity to a giant core would be crucial for a node's capability to deliver its tasks.

Robustness of networks under the giant-component based failure model has been exten-

sively analyzed in the case of *single* networks [5, 64, 65]. The focus has recently been shifted towards *interdependent* networks with the work of Buldyrev et al. [9], where robustness of two interdependent networks, both operating under the giant-component based intra-dependence rule, was studied. Their model, and most works that follow, are unable to capture the true nature of a cyber-physical network, where the cyber-network and the physical-network should obey a different set of rules determining their intra-dependencies.

We define the structure of the network B through its *degree distribution*, namely the probabilities $\{d_k,\ k = 0, 1, \ldots\}$ that an arbitrary node in B has degree k; clearly, we need to have $\sum_{k=0}^{\infty} d_k = 1$. In particular, each node $b_1, \ldots, b_N$ is assigned a degree drawn from the distribution $\{d_k\}_{k=0}^{\infty}$ independently from any other node. Once the degree sequence, $\text{degree}(b_1), \ldots, \text{degree}(b_N)$, of the network is determined, network B is constructed by selecting *uniformly at random* a graph among all graphs on N nodes with the given degree sequence; see [65, 123, 124] for details of such constructions. This class of networks is known in the literature as the *configuration model* or *random graphs with arbitrary degree distribution*. Degree distribution is often regarded as the core property defining a graph, and random networks with arbitrary degree distributions are extensively used as a starting point in the literature on robustness of complex networks.

Interdependent System Model. For simplicity, the interdependence across the two networks is assumed to be one-to-one; i.e., every node in the cyber-network is dependent upon and supports a single node in the physical network, and vice versa; see Figure 6.2. More precisely, we assume that for each $i = 1, \ldots, N$, nodes a_i and b_i are dependent on each other meaning that if one fails, the other will fail as well. Although simplistic, the one-to-one interdependence model is considered to be a good starting point and has already provided useful insights in similar settings [9]; more complicated interdependence models shall be considered in future work including regular allocation strategy, i.e., each node in A is connected to k nodes in B and vice versa, or a more general case where some nodes do not have interdependent links and can function even without any support from the other network.

With these in mind, we are interested in understanding the dynamics of cascading failures in this interdependent system, where failures are initiated by removing a $(1-p)$-fraction of nodes, selected *randomly*, from network A . As explained in Figure 6.1, we assume an asynchronous cascade model, where intra-propagation and inter-propagation of failures are considered in a sequential manner. At any stage $t = 1, 2, \ldots$ of the cascade process, a node a_i in network A will still be functioning if and only if (i) its current flow at time t is less than its capacity; *and* (ii) its counterpart b_i in network B is still functioning (which is equivalent to b_i being contained in the largest connected subgraph of B). Similarly, a node b_j in network B survives cascade step t if and only if i) it belongs to largest connected component of B at time t; and (ii) its counterpart a_j in network A is still functioning (which is equivalent to a_j carrying a flow at time t that is less than its capacity).

Since the cascade process is monotone, a steady-state will eventually be reached, possibly after all nodes have failed. Let $\mathcal{N}_{\text{surviving}} \subset \{1, \ldots, N\}$ be the set of node id's that are still functioning at the steady state. In other words, the surviving interdependent system will consist of nodes $\{a_i : i \in \mathcal{N}_{\text{surviving}}\}$ where each a_i has more capacity than its flow and $\{b_i : i \in \mathcal{N}_{\text{surviving}}\}$ that constitute a connected subgraph of (the giant component of) network B. The primary goal of this paper is to derive the *mean* fraction of nodes that survive the cascades as a function of the initial attack size $1 - p$, in the asymptotic limit of large network size N. More precisely, we would like to characterize $S(p)$ defined as

$$S(p) := \lim_{N \to \infty} \frac{\mathbb{E}\left[|\mathcal{N}_{\text{surviving}}(p)|\right]}{N}$$

Note that this definition of $S(p)$ represents the same quantity as $n_\infty(p)$ in equation 3.1, except that here we consider the mean fraction of nodes instead of lines survived at the steady-state. In what follows, we present our main result that allows computing $S(p)$ under any degree distribution $\{d_k\}_{k=0}^{\infty}$ of the cyber-network B, any load-(free-space) distribution $P_{LS}(x, y)$ of the physical network A, and under any attack size $0 \leq 1 - p \leq 1$. This is followed in Section 6.4 by a numerical study that demonstrates the accuracy of our analysis even with finite N, and

presents insights on how the robustness of an interdependent cyber-physical system can be improved by careful allocation of available resources (e.g., node capacities and degrees).

6.3 Main results

Our main result is presented next. The approach is based on recursively deriving the *mean* fraction of surviving nodes from both networks at each stage $t = 1, 2, \ldots$ of the cascade process. The cascade process starts at time $t = 0$ with a random attack that kills $1 - p$ fraction of the nodes from network A. As mentioned earlier, we assume an asynchronous cascading failure model where at stages $t = 1, 3, \ldots$ we consider the failures in network A and in stages $t = 2, 4, \ldots$ we consider the failures in network B. In this manner, we keep track of the subset of vertices $A_1 \supset A_3 \supset \ldots \supset A_{2i+1}$ and $B_2 \supset B_4 \supset \ldots \supset B_{2i}$ that represent the functioning (i.e., surviving) nodes at the corresponding stage of the cascade. We let f_{A_i} denote the *relative* size of the surviving set of nodes from network A at stage i, i.e.,

$$f_{A_i} = \frac{|A_i|}{N}, \quad i = 1, 3, 5, \ldots$$

We define f_{B_i} similarly as

$$f_{B_i} = \frac{|B_i|}{N}, \quad i = 2, 4, 6, \ldots$$

Our main result, presented next, shows how these quantities can be computed in a recursive manner.

Theorem 5. *Consider an interdependent system as described in Section 6.2, where the load and free-space values of nodes $a_1, \ldots, a_N$ are drawn independently from the distribution p_{LS}, and network B is generated according to the configuration model with degree distribution $\{d_k\}_{k=0}^{\infty}$; i.e., we have $\mathbb{P}[\text{degree of node } b_i = k] = d_k$ for each $k = 0, 1, \ldots$ and $i = 1, \ldots, N$. Let mean degree be denoted by $\langle d \rangle$, i.e., let $\langle d \rangle = \sum_{k=0}^{\infty} k d_k$. With $f_{B_0} = p_{B_0} = p$, $f_{A_{-1}} = 1$, and $Q_{-1} = 0$, the relative size of the surviving parts of network A and B at each stage of*

the cascade, initiated by a random attack on $1-p$ fraction of the nodes, can be computed recursively as follows for each $i = 0, 1, \ldots$

$$p_{A_{2i+1}} = \frac{f_{B_{2i}}}{f_{A_{2i-1}}} \tag{6.2}$$

$$Q_{2i+1} = Q_{2i-1} + \min\left\{x \in (0,\infty] : \frac{\mathbb{P}\left[S > Q_{2i-1} + x\right]}{\mathbb{P}\left[S > Q_{2i-1}\right]}(x + Q_{2i-1} + \mathbb{E}\left[L | S > x + Q_{2i-1}\right]) \geq \frac{Q_{2i-1} + \mathbb{E}\left[L | S > Q_{2i-1}\right]}{p_{A_{2i+1}}}\right\} \tag{6.3}$$

$$f_{A_{2i+1}} = f_{A_{2i-1}} \cdot p_{A_{2i+1}} \cdot \mathbb{P}\left[S > Q_{2i+1} \mid S > Q_{2i-1}\right] \tag{6.4}$$

$$p_{B_{2i+2}} = p_{B_{2i}} \frac{f_{A_{2i+1}}}{f_{B_{2i}}} \tag{6.5}$$

$$u_{2i+2} = \max\left\{u \in [0,1] : u = 1 - \sum_{k=0}^{\infty} \frac{k d_k}{\langle d \rangle}(1 - u \cdot p_{B_{2i+2}})^{k-1}\right\} \tag{6.6}$$

$$f_{B_{2i+2}} = p_{B_{2i+2}}\left(1 - \sum_{k=0}^{\infty} d_k \left(1 - u_{2i+2} \cdot p_{B_{2i+2}}\right)^k\right) \tag{6.7}$$

The notation used in Theorem 5 is summarized in Table 6.1. In these iterations, it is assumed that if at any stage i, it happens to be the case that no $x < \infty$ satisfies the inequality at (6.3), we set $Q_{2i+1} = \infty$. It is then understood that the entire network A (and thus B) have failed, and we get $f_{A_{2i+1}} = f_{B_{2i+2}} = 0$. Similarly, it can be seen that the equality in (6.6) always holds with $u = 0$. Thus, if at any stage i, there is no $u > 0$ satisfying the equality in (6.6), we will get $u_{2i+2} = 0$ leading to $f_{B_{2i+2}} = 0$; i.e., the entire network B (and thus A) will have collapsed.

A_i	set of surviving nodes in network A at stage $i = 1, 3, 5, \ldots$
B_i	set of surviving nodes in network B at stage $i = 2, 4, 6, \ldots$
$f_{A_{2i+1}}$	fraction $\lvert A_{2i+1}\rvert/N$ of surviving nodes in A at stage $2i+1$
$f_{B_{2i+2}}$	fraction $\lvert B_{2i+2}\rvert/N$ of surviving nodes in B at stage $2i+2$
Q_{2i+1}	extra load per surviving node in A at stage $2i+1$
$p_{A_{2i+1}}$	prob. of a node in A_{2i-1} surviving *inter*-failures at stage $2i$
$1 - p_{B_{2i+2}}$	*equivalent* prob. of random attack to B that gives B_{2i+2}
u_{2i+2}	auxiliary variable used in computing $f_{B_{2i+2}}$

Table 6.1: Key notation in the analysis of cascading failures

As mentioned before, our goal is to obtain the *final* system size, i.e., the relative size of the surviving nodes at the steady-state. In view of the one-to-one interdependence model, the surviving size of the networks A and B will be the same at the steady-state. Thus, we conclude that

$$S(p) = \lim_{i\to\infty} f_{A_i} = \lim_{i\to\infty} f_{B_i}.$$

Next, we provide an outline of the proof, while the full details are available in Appendix. In [23], we already analyzed the cascade dynamics and derived the final system size in a single flow carrying network (similar to network A in our analysis), when $1-p$ fraction of its nodes are randomly removed; the result enables computing the final system size in terms of the initial attack size $1-p$, as well as the load and free space distribution $P_{LS}(x,y)$. The results established in [23] are incorporated in the recursions above through expression (6.3) that allows us to calculate, in a recursive manner, the extra load that each of the surviving nodes at a particular stage will be carrying in addition to their initial load.

According to the failure propagation model described at the beginning of this section, at odd stages failures from network B can propagate to network A, causing a fraction of nodes to be removed. As explained in details in Appendix, given that the intra-failure dynamics of network B is completely independent from network A, the impact of the failures in B to network A will be equivalent to a *random* attack launched on A. In addition, at each odd stage $t = 2i-1$, $i = 1, 2, \cdots$, we can treat the remaining part of network A as a new physical network A_{2i-1}, with the appropriately updated size and load-'free-space' distribution. Thus, the random removal of nodes caused by failures in network B (through the one-to-one interdependency links) from last cascade stage can be viewed as a new random attack to A_{2i-1} that keeps only $p_{A_{2i+1}}$ fraction of its nodes alive. Then following a similar approach, we can compute the size of network A at the next stage $2i+1$, i.e., $f_{A_{2i+1}}$. An important observation is the need to update the load and free-space distributions for each new network A_{2i+1} to incorporate the facts that the surviving nodes in A_{2i+1} are added with Q_{2i-1} amount of extra load, and at the same time the free-space of each surviving node must be at least Q_{2i-1}. We show in the detailed proof

in Appendix that the changes of the distribution can be represented by the initial load and free-space distribution with Q_{2i+1} representing the extra load in each stage. In other words, each time failures propagate between the two networks, network A will shrink to a group of nodes that have a higher free space and that are now carrying more load. The fractional size of this surviving subset of nodes at each time stage can be computed via the equivalent attack size $p_{A_{2i+1}}$ (caused by failures in network B propagated via the one-to-one dependent links), extra load Q_{2i+1} and the load free-space distribution $P_{LS}(x, y)$; see (6.2)-(6.4).

Following the same approach, in network B we treat each new failure that comes from network A as a new random attack (or failure) on the existing network B_{2i+2}. For a node in network B to function, it must belong to the largest connected (i.e., giant) component, so actually the functioning network B_{2i+2} at time stage $t = 2i + 2, i = 0, 1, 2, \cdots$ is the giant component after the random attack propagated from network A. A key insight here is that the sequential process of applying a first random attack on the cyber-network, then computing the giant component, and then applying a second random attack and then computing the giant component is *equivalent* to (in terms of the fractional size of the set of nodes that survives) the process where the second random attack is applied directly after the first one without computing the giant component; e.g., see [9]. This way, the result of a series of random attack/giant-component calculation processes can be emulated by a single random attack/giant-component calculation, with an appropriately calculated *equivalent* random attack size. In our calculations, this *equivalent* attack size for stage $2i + 2$ is represented by $1 - p_{B_{2i+2}}$ and can be computed recursively as given in (6.5). This formula is based on treating all *new* failures propagated from network A in the following time stage as the new random attack size launched on B, which is then used to update the equivalent attack size $1 - p_{B_{2i+2}}$ that will be used to emulate the entire cascade sequence up until that stage. Then, the size of network B_{2i+2}, namely the size of the giant component after randomly removing $(1 - p_{B_{2i+2}})$-fraction of nodes, can be computed using the technique of generating functions [9, 13, 64–66]. The formulas that give the network size $f_{B_{2i+2}}$ at each time stage $i = 0, 1, \ldots$ are presented at (6.6) and (6.7).

Once we know how to compute the surviving network sizes $f_{A_{2i+1}}$ and $f_{B_{2i+2}}$ at each stage, the propagation of failures between the two networks is seen to be governed via (6.2) and (6.5) that reveal how the key quantities p_{A2i+1} and $p_{B_{2i+2}}$ used in computing $f_{A_{2i+1}}$ and $f_{B_{2i+2}}$, respectively, need to be updated based on the result of the last cascade stage. Collecting, a thorough analysis that reveals a full understanding of the system behavior and robustness during the failure process is presented in equations (6.2)-(6.7).

6.4 Numerical results

In this section, we confirm our analytic results through numerical simulations under a wide range of parameter choices, with a particular focus on checking the accuracy of the results when the network size N is finite.

For physical networks carrying a certain flow (i.e., network A in our analysis), we consider different combinations of probability distributions for the load and free-space variables. Throughout, we consider three commonly used families of distributions: i) Uniform, ii) Pareto, and iii) Weibull. These distributions are chosen here because they cover a wide range of commonly used and representative cases. In particular, uniform distribution provides an intuitive baseline. Distributions belonging to the Pareto family are also known as a *power-law* distributions and have been observed in many real-world networks including the Internet, the citation network, as well as power systems [79]. Weibull distribution is widely used in engineering problems involving reliability and survival analysis, and contains several classical distributions as special cases; e.g., Exponential, Rayleigh, and Dirac-delta.

The corresponding probability density functions are defined below for a generic random variable L.

- Uniform Distribution: $L \sim U(L_{\min}, L_{\max})$. The density is given by

$$p_L(x) = \frac{1}{L_{\max} - L_{\min}} \cdot \mathbf{1}\left[L_{\min} \leq x \leq L_{\max}\right]$$

- Pareto Distribution: $L \sim Pareto(L_{\min}, b)$. With $L_{\min} > 0$ and $b > 0$, the density is given by

$$p_L(x) = L_{\min}^b b x^{-b-1} \mathbf{1}\left[x \geq L_{\min}\right].$$

To ensure that $\mathbb{E}[L] = bL_{\min}/(b-1)$ is finite, we also enforce $b > 1$. Distributions belonging to the Pareto family are also known as a *power-law* distributions and have been extensively used in many fields including power systems.

- Weibull Distribution: $L \sim Weibull(L_{\min}, \lambda, k_w)$. With $\lambda, k_w, L_{\min} > 0$, the density is given by

$$p_L(x) = \frac{k_w}{\lambda}\left(\frac{x - L_{\min}}{\lambda}\right)^{k_w - 1} e^{-\left(\frac{x-L_{\min}}{\lambda}\right)^{k_w}} \mathbf{1}\left[x \geq L_{\min}\right].$$

The case $k_w = 1$ corresponds to the exponential distribution, and $k_w = 2$ corresponds to Rayleigh distribution. The mean is given by $\mathbb{E}[L] = L_{\min} + \lambda\Gamma(1 + 1/k_w)$, where $\Gamma(\cdot)$ is the gamma-function given by $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$.

As explained in Section 6.2.2, the cyber-network where a node is only functional when it belongs to the giant component (i.e., network B in our analysis) is generated according to the configuration model with degree distribution $\{d_k\}_{k=0}^\infty$. In the simulations, we consider two representative cases given below:

- Erdős-Rényi (ER) network model [125–127]. This corresponds to having the degree distribution d_k follow a Binomial distribution, i.e., $d_k \sim \text{Binomial}(N-1; \frac{\langle d\rangle}{N-1})$; as before $\langle d\rangle$ gives the mean node degree.

- The scale-free (SF) network model [5]. We consider the case where the degree distribution $\{d_k\}_{k=0}^\infty$ is a *power-law* with *exponential cut-off*, which was observed [128] in many real networks including the Internet; i.e., we have

$$d_k = \begin{cases} 0 & \text{if } k = 0 \\ \frac{1}{\text{Li}_\gamma(e^{-1/\Gamma})} k^{-\gamma} e^{-k/\Gamma} & \text{if } k = 1, 2, \cdots, \end{cases} \tag{6.8}$$

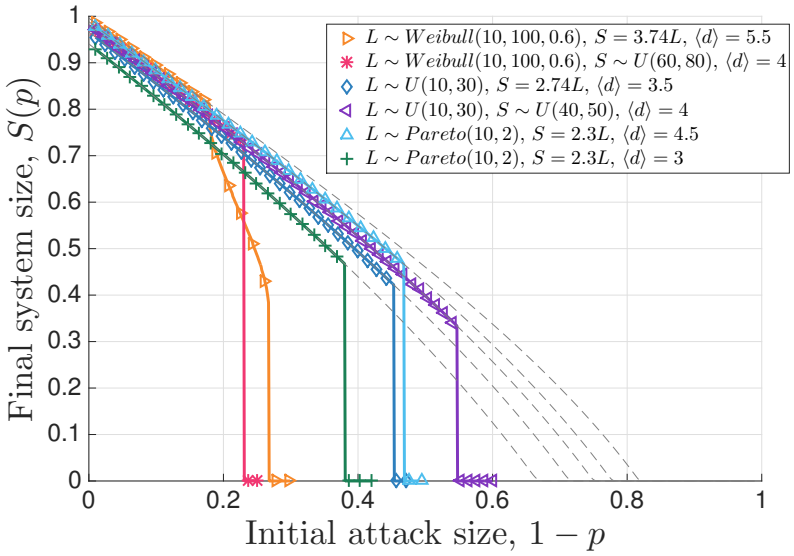


Figure 6.3: *Final system size under different network settings, including different load-free space distributions in the physical network and different mean degree in the cyber network modeled by an ER network. Analytic results are represented by lines, whereas simulation results are represented by symbols (averaged over 100 independent runs). We see that in each case theoretical results match the simulation results very well. Gray dashed lines show the robustness behavior of a* single *cyber-network (i.e., not interdependent with a physical network) for comparison.*

where γ is the power exponent, Γ is the cut-off point, and $\mathrm{Li}_m(z) := \sum_{k=1}^{k=\infty} z^k k^{-m}$ is the normalizing constant.

We remind that although we restrict our attention to these special cases in the simulations, our analysis applies under more general degree distributions as well.

6.4.1 Fiber network coupled with ER network

The Erdős-Rényi graph is one of the most basic and widely used network models and often serve as a starting point in simulations. In our study, we start with N nodes, and connect each pair of vertices with an edge with probability $\langle d \rangle/(N-1)$ independently from each other. When N is large, this is equivalent to generating the network via the configuration model using a *Poisson* degree distribution with mean $\langle d \rangle$.

First, we confirm our main result presented in Sec. 6.3 concerning the final system size $S(p)$, i.e., the mean fraction of surviving nodes at the end of cascading failures initiated by

a random attack that removes $1-p$ fraction of nodes in network A. In all simulations, we fix the number of nodes in both networks at $N = 10^5$, and for each set of parameters being considered (i.e., the distribution $p_{LS}(x, y)$, the attack size $1-p$ in network A, and the mean degree $\langle d \rangle$ in network B), we run 100 independent experiments. The results are shown in Figure 6.3 where symbols represent the *empirical* value of the final system size $S(p)$ (obtained by averaging over 100 independent runs for each data point), and lines represent the analytic results computed via (6.2)–(6.7). We see that theoretical results match the simulations very well in all cases[1]. This suggests that although asymptotic in nature, our main result can still be helpful when the network size N is finite. The specific distributions used in Figure 6.3 are as follows: From left to right, we have i) in network A (the physical network), L is Weibull with $L_{\min} = 10, \lambda = 100, k_w = 0.6$ and $S = \alpha L$ with $\alpha = 3.74$; in network B (the cyber network) the mean degree $\langle d \rangle = 5.5$; ii) in network A, L is Weibull with $L_{\min} = 10, \lambda = 100, k_w = 0.6$ and S is Uniform over $[60, 80]$; in network B $\langle d \rangle = 4$; iii) L is Uniform over $[10, 30]$ and and $S = \alpha L$ with $\alpha = 2.74$; in network B $\langle d \rangle = 3.5$; iv) L is Uniform over $[10, 30]$ and S is Uniform over $[40, 50]$; $\langle d \rangle = 4$; v) L is Pareto with $L_{\min} = 10$, $b = 2$, $S = \alpha L$ with $\alpha = 2.3$; $\langle d \rangle = 4.5$; vi) L is Pareto with $L_{\min} = 10$, $b = 2$, $S = \alpha L$ with $\alpha = 2.3$; $\langle d \rangle = 3$.

In Figure 6.3, gray dashed lines correspond to the case where a single cyber network (with the same parameters used in Figure 6.3) is attacked. We see that interdependent systems can be significantly more vulnerable to attacks as compared to single networks. An interesting observation is that despite their vulnerability at *large* attack sizes, the robustness of interdependent systems (quantified by the final system size $S(p)$) overlaps with the single cyber network case up until the attack size exceeds a certain level. This indicates the possibility of designing an interdependent system with the same level of robustness as a single network as long as attacks or failures that exceed a certain size are ruled out.

The plots in Figure 6.3 show how different load-free space distributions in network A as well

[1]We remark that when loads follow a Uniform distribution, it is sufficient to have a few thousand nodes in the network in order to observe the match between simulations and analytic results (which are asymptotic in nature). However, larger networks with around hundred thousand nodes are needed when highly-variable distributions such as Pareto are used to generate the load values.

as the mean degree in network B affect the system behavior. For example, with the mean degree of network B is fixed to $\langle d \rangle = 4$, the two different cases considered in Figure 6.3, one where the initial loads in network A follow a Weibull distribution (magenta asterisk) and the other where the initial loads follow a Uniform distribution (purple triangle) lead to vastly different system behavior against attacks. When load in network A follows Weibull distribution, the final system size drops to zero at a point where the attack size is around 0.23, meaning that any random attack that kills more than 23% of the nodes will destroy the entire system. On the other hand, if the load and free space follows Uniform distribution, the system is quite robust and can sustain initial attack sizes up to 0.55 without collapsing. Similarly, when we fix the distribution in network A, we can see the effect of mean degree in the cyber network on system robustness: when initial load in physical network follows Pareto$(10, 2)$ distribution, and free space is given by $S = \alpha L$ with $\alpha = 2.3$, we see that increasing mean degree of network B from $\langle d \rangle = 3$ (green cross) to $\langle d \rangle = 4.5$ (light blue triangle) leads to a substantial increase on the final system size at *all* attack sizes; i.e., the interdependent CPS becomes more robust. This is intuitive since higher $\langle d \rangle$ values lead to a cyber-network B with higher levels of connectivity enabling the entire CPS to sustain larger attacks while maintaining a larger fraction of nodes in its giant component.

An interesting observation from Figure 6.3 is that in all cases, the final drop of the system size to zero takes place through a *first-order* (i.e., discontinuous) transition[2], making it difficult to predict system behavior from previous data (in response to attacks with larger than previously observed size). In fact, this abrupt failure behavior is reminiscent of the real-world phenomena of unexpected large-scale system collapses; i.e., cases where seemingly identical attacks/failures leading to entirely different consequences. We also see that our model can lead to a rich set of behaviors to increasing attack sizes. For instance, when the initial load follows a Weibull distribution, depending on the parameters, it is possible to observe an abrupt first-

[2]The nomenclature concerning the order of transitions is adopted from the studies on phase transition in Physics; simply put, first (resp. second) order transitions are associated with *discontinuous* (resp. continuous) variations.

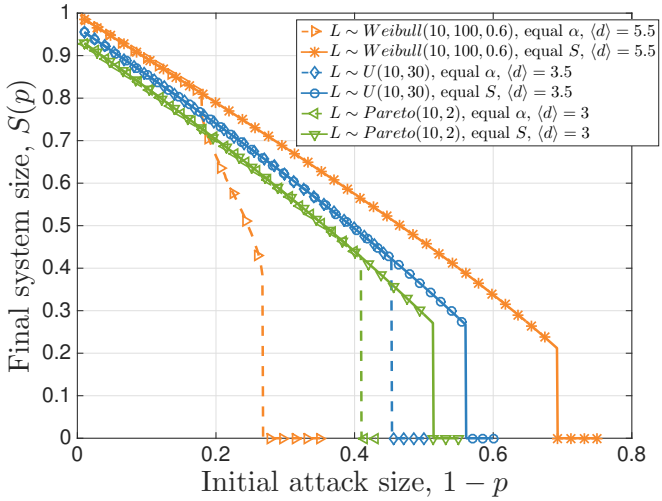


Figure 6.4: *Final system size under equal free space (solid lines with symbols) or equal tolerance factor (dashed lines with symbols) when network B is a ER graph with fixed mean degree. The symbols are empirical results over 100 independent runs on network size* $N = 10^5$*, and lines (dashed or solid) represent analytic results. We can see in all cases equal free space greatly improves system robustness by allowing the system to sustain a larger initial attack size and still not collapsing.*

order transition with no prior indication of system collapse at smaller attack sizes (magenta asterisk), as well as a first-then-second order transition (orange triangle) before the system size drops to zero through a final first-order transition. These behaviors are due to the intrinsic characters of different distributions, and should be considered in designing CPS where the physical network may be governed by different flow distribution types.

From a design perspective, it is of interest to understand how the robustness of the interdependent system can be improved or even maximized under certain constrains. To gain insights on this, we fix the mean degree in network B (the cyber network), and explore the effect of the allocation (i.e., distribution) of node capacities in the physical network. A key determining factor of system robustness is expected to be the free-space distribution as it specifies the extra load a node can receive from the failed ones before it fails due to overloading. The vast majority of the literature and most real world applications employ a *linear* free-space allocation scheme where the free-space assigned to a node is set to be a fixed proportion of its initial load. In other words, it is assumed that $S = \alpha L$, where α is the *tolerance factor* and is usually a fixed value [59, 77, 84, 85] used for the entire network. We already showed in [23] that

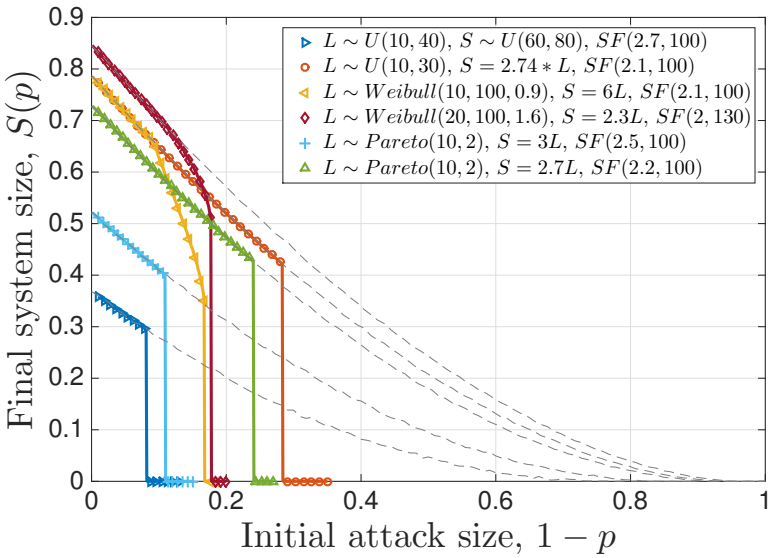


Figure 6.5: *Final system size under different network settings, including different load-free space distributions in the physical network and different exponent in the scale-free cyber network. Analytic results are represented by lines, whereas simulation results are represented by symbols (averaged over 100 independent runs). The gray dashed line represents the case when a single cyber network is attacked. In all cases, theoretical results match the simulation results well.*

in a single flow-carrying network, allocating every node exactly the same free-space leads to a higher robustness (at any attack size $1-p$) than the commonly used setting of equal tolerance factor (with the comparison made when the total free-space in the entire network is fixed). In fact, in the single network case, the robustness is shown to be *maximized* when all nodes receive the same free space.

Our numerical simulations, presented in Figure 6.4, shows that the above conclusion still applies in interdependent networks. Namely, assigning every node the same free space provides a much better overall system robustness as compared to the widely used setting of equal tolerance factor (i.e., linear free-space allocation). To provide an overall evaluation of the system robustness, we define the critical attack size $1-p^\star$ as the minimum attack size that breaks down the whole system. Thus, the larger $1-p^\star$ is, the more robust will the system be since it can sustain larger attacks. In Figure 6.4, the comparison between the equal free-space and equal tolerance factor allocations are made with the mean free space $\mathbb{E}[S]$ being fixed (i.e., the total free space in the network is constrained). We see that compared to the equal tolerance factor scheme, the equal free-space allocation enables the system to sustain much

larger attacks. In fact, in the case of Weibull distribution, the robustness is almost 2.5 times higher in the case of equal free space as compared to the case with equal tolerance factor; i.e., $1 - p^\star = 0.7$ vs. $1 - p^\star = 0.28$.

6.4.2 Flow-carrying network coupled with SF network

Although the ER graph constitutes a simple and useful network model, networks in most real-world applications might have significantly different structure and robustness behavior against attacks. For instance, scale-free networks (SF model) were shown [129] to exhibit fundamentally different robustness behavior with ER networks; the former is very robust against random attacks but fragile against *targeted* attacks, while the situation is exactly the opposite for the latter. In order to better understand the impact of the topology of the cyber-network on the overall robustness of an interdependent CPS, we consider in this section the case where the cyber network (network B) has a power-law degree distribution with exponential cutoff. In addition to being observed in many real-world networks including the Internet [128], power-law distributions with exponential cut-off also ensure that all moments of the node degree are *finite*, which helps certain convergences take place faster (i.e., with smaller N).

In Figure 6.5, we verify our analytic results when network B (cyber network) has a degree distribution in the form of a power-law with exponential cut-off; this is denoted by $SF(\gamma, \Gamma)$, where γ is the power exponent and Γ is the cut-off parameter given at (6.8). In all cases, we fix the number of nodes in both networks to be $N = 10^6$, and consider several different load-'free space' distributions in network A and different (γ, Γ) values for network B (while noting that in real-world networks, it is often observed that $2 < \gamma < 3$). The simulation results are obtained by averaging over 100 independent experiments for each data point and it is seen that they are in very good agreement with the analytic results.

Next, we seek to obtain an overall understanding of how the free-space allocation in the physical network together with the topology of the cyber network (ER vs. SF model) affect the system robustness. With the discussion from Section 6.4.1 in mind, we consider the widely

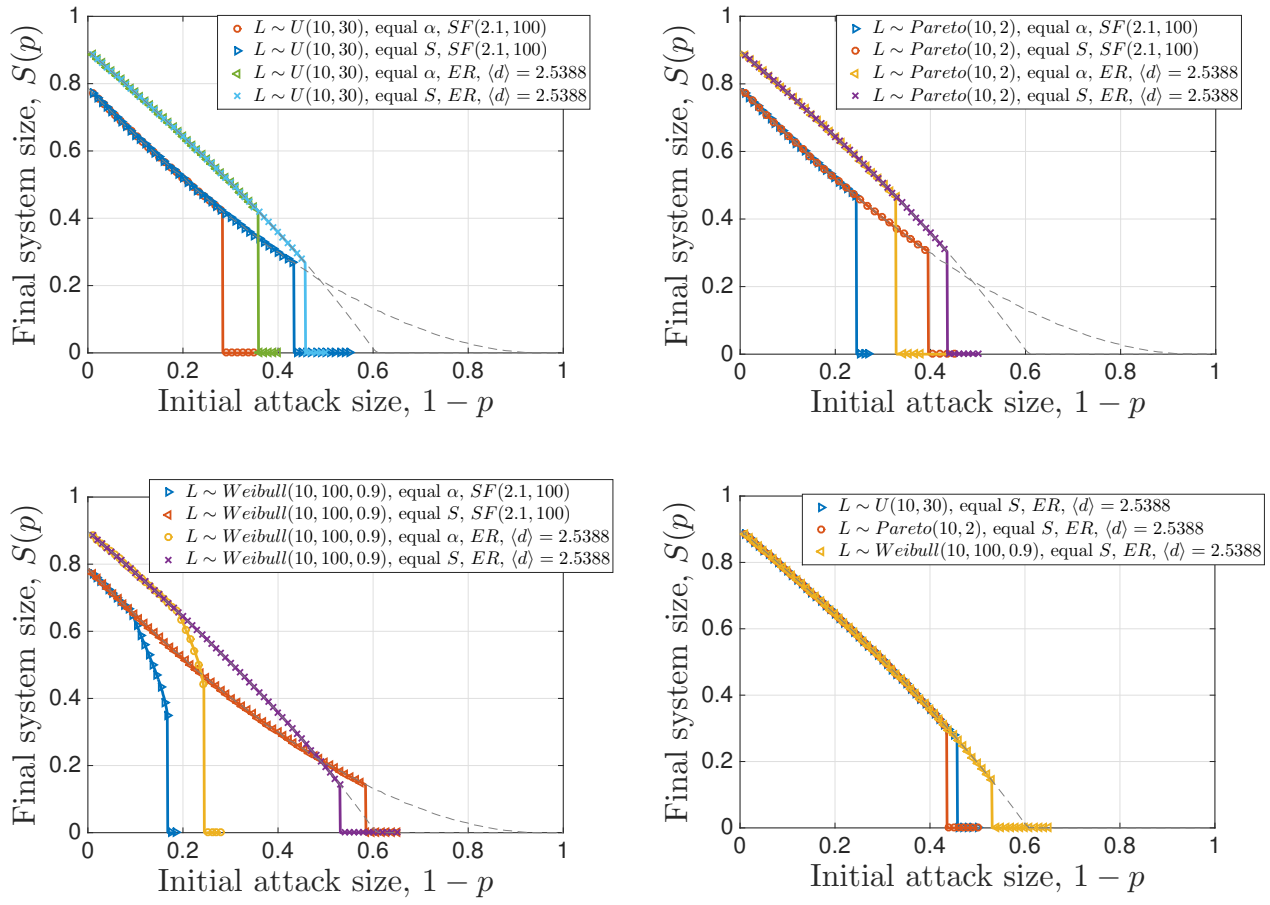


Figure 6.6: *Comparison of final system size when equal tolerance factor (equal α) and equal free space (equal S) schemes are used. The mean value of free space is kept the same, as well as the mean degree in SF and ER networks. In all cases, equal S outperform the widely used equal α scheme. The effect of topology in the cyber network is not unitary: in some cases ER leads to better robustness, while in other cases SF is better, contradicting the results [5] concerning the robustness of single networks. To compare with the case where a single cyber network is randomly attacked, gray dashed lines show the final system size $S(p)$ of a single ER and SF network (with the same parameters as above).*

used equal tolerance factor allocation (equal α), where the free-space S is a fixed factor α of the load on a node (i.e., $S = \alpha * L$) and the equal free-space allocation scheme (equal S) that was shown [23] to be optimal in a single physical network. For fairness, all comparisons are made under the same initial load distribution, and with the mean free-space in network A and the mean node degree in network B being fixed.

The results are shown in Figure 6.6. We can see that no matter how the initial load is distributed, i.e., whether it's Uniform, Pareto or Weibull, and despite of the structure of the cyber network being SF network or ER network, equal free-space allocation can greatly improve system robustness as compared to the equal tolerance factor allocation. We observe that when all nodes in network A are given the same free-space, the overall interdependent CPS can sustain a much larger initial attack size without collapsing; i.e., it has a much larger critical attack size. For example in the case of Weibull distributed load with SF network, the system can only take around 16.8% of initial attack size when using equal α, but can sustain a initial attack that removes 58% of the nodes when equal S is used, making the system about 3 times more robust in terms of the critical attack size.

We also see in Figure 6.6 that the topology of the cyber network affects the robustness of the interdependent CPS in an intricate way, with some cases showing the exact opposite of what would have been expected from the results on single networks. In particular, SF networks are known [5] to be more robust than ER networks against random attacks. This is often attributed to the fact that SF networks typically have a few nodes with very high degrees and the network will likely contain a large connected component unless these high-degree nodes are removed (which is unlikely to happen if the attack is *random*); this dependence on a few nodes is exactly what makes SF networks very fragile against a *targeted* attack. In the case of the interdependent CPS model, we see that the comparison of the overall robustness between the cases where they cyber network is SF or ER is a much more complicated matter. In fact, depending on the load-'free-space' distribution in the physical network, the cyber network being SF does *not* always lead to a better robustness than the case with ER. For example, in

the upper two plots in Figure 6.6 where the initial load is Uniform and Pareto, respectively, the cases with the ER network leads to a better robustness than that with SF. In the bottom left picture where the initial load in the physical networks is Weibull, the situation is even more intricate. With equal α, the case where the cyber-network is ER leads to a better robustness, while SF network performs better (in terms of the critical attack size) under the equal-S allocation. This shows that an integrated CPS can not be designed in the most robust way by considering the physical and cyber counterparts separately. Instead, a holistic design approach is needed where the robustness of the CPS as a whole is considered.

An intuitive explanation for these findings can be obtained from the comparison of the robustness of a single SF network and an ER network, which is shown in gray dashed lines in Figure 6.6. From this, we see that the SF network is more robust than the ER network *only* in the sense that its "critical" attack size, after which the final system size is zero, is larger than that of the ER network. However, for any attack size smaller than a certain point (around $1-p=0.5$), the ER network has a larger final system size than the SF network. This can be the underlying reason for seeing different comparisons with regard to the robustness of interdependent CPSs. If the physical network that the cyber-network is interdependent with has a *small* critical attack size (i.e., it is fragile), then the interdependent CPS will be more robust when the cyber network is ER as compared to case when it is SF. However, if a robust physical network with *large* critical attack size is made inter-dependent with a cyber network, then the CPS is more robust when the cyber-network is SF.

6.5 Simulation results under global-local combined flow redistribution model

In this section, we check via simulations the robustness of an interdependent CPS where the physical network has a given topology and redistribution of flow (from failed nodes) is done, at least in part, according to this topology. To this end, we consider *global-local combined*

redistribution model [120], where μ fraction of load will go to the neighbors of a failed node, and $1-\mu$ fraction of load will go to all remaining nodes in the network. The intra-dependency in the cyber network and the inter-dependence model between the two networks remain the same. With this approach, we recover the model analyzed in our paper when $\mu = 0$, while setting $\mu = 1$ leads to a fully topology-based redistribution model in the physical network.

In Figure 6.7, we present simulation results showing the robustness of an interdependent CPS under different μ values. For simplicity, we assume the load-carrying physical network has an underlying topology characterized by an ER graph with mean degree $\langle d \rangle = 2.5388$. The network size is taken to be $N = 10^5$ and the coupled cyber network is also taken to be an ER graph with the same parameters (though it is generated independently from the physical network). The load carried by each node in the physical network follows uniform distribution $U(10, 30)$, and free space follows either equal-α ($\alpha = 2.74$) or equal-S ($S = 54.8$) allocations.

We see from Figure 6.7 that as μ changes from 0 to 1, i.e., when the physical network gradually changes from a fully global redistribution model ($\mu = 0$) to a fully local redistribution model ($\mu = 1$), the robustness of the whole system decreases. However, the qualitative behavior of the robustness remains unchanged under different μ values. In particular, in all cases we observe a first-order (i.e., discontinuous) transition at the critical attack size when final system size $S(p)$ drops to zero. Furthermore, we see that in all cases the equal-S allocation of capacities outperforms (in terms of robustness) the commonly used equal-α allocation. Concluding, these simulation results suggest that the mean-field approach used in our analysis (i.e., the case with $\mu = 0$) is able to capture well the qualitative behavior of final system size for all μ values.

We should note that when $\mu = 1$, i.e. a fully local redistribution model is deployed, the difference between the equal S and equal α allocation scheme is greater when the load and free space distribution has larger variance. This is illustrated further in Figure 6.8, where the cyber network is kept the same with Figure 6.7, but the variance of load distribution is greater with $L\ U[5, 75]$.

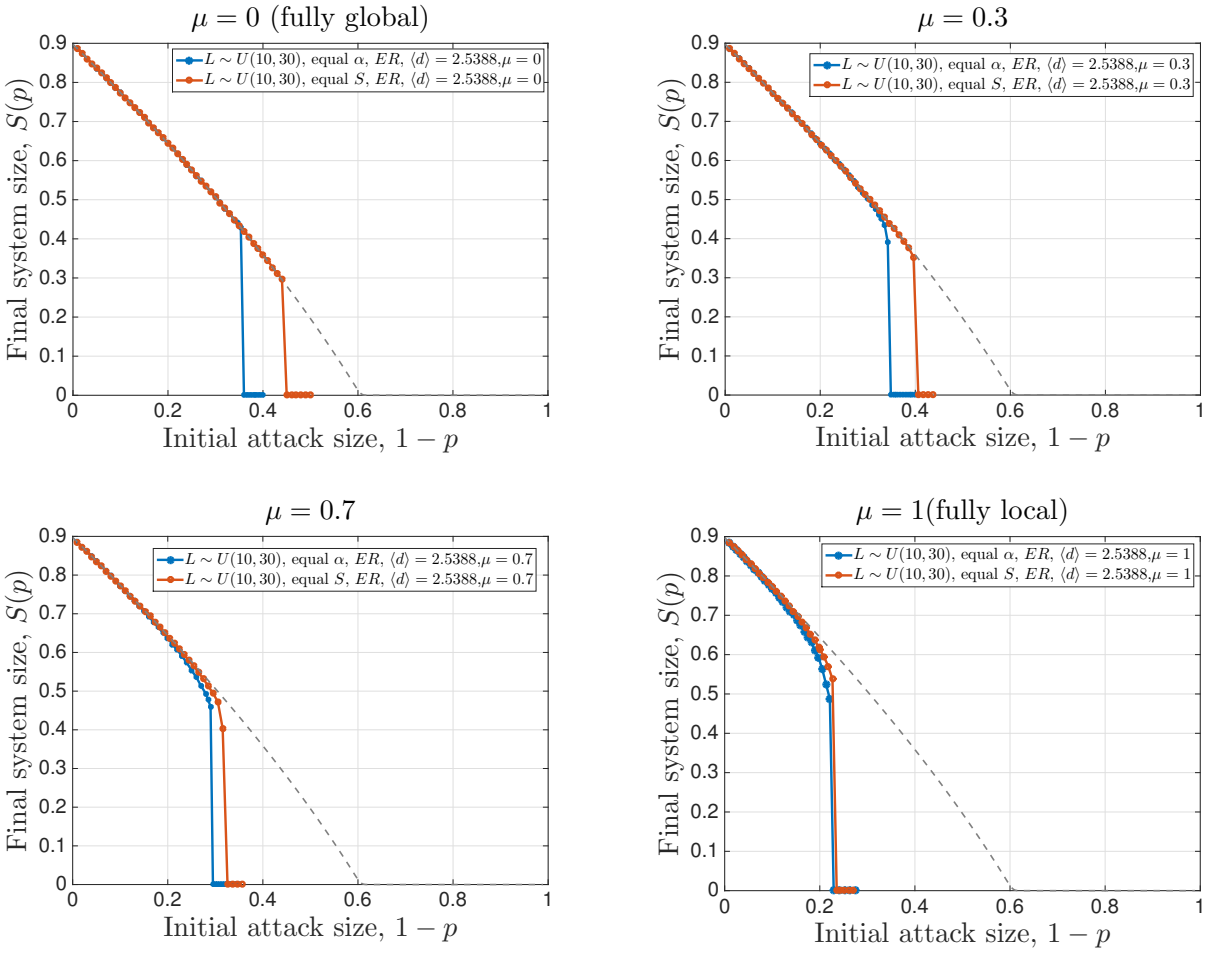


Figure 6.7: *Physical network adopts the global-local redistribution rule under ER topology, with μ denoting the fraction of flow redistributed locally. The gray dashed line represents the case when a single ER graph is randomly attacked. In all cases, we see that equal-S allocation outperforms the equal-α allocation, meaning that the qualitative behavior of the robustness remains unchanged under different μ values.*

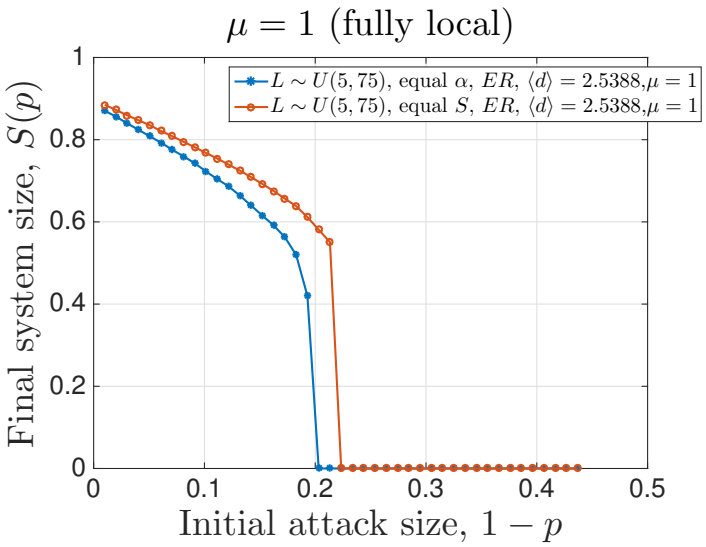


Figure 6.8: *Physical network adopts the global-local redistribution rule under ER topology, with μ denoting the fraction of flow redistributed locally. In the case when $\mu = 1$, a fully local distribution is deployed, the difference between equal S and equal α is larger when the variance of the load distribution is greater.*

6.6 Chapter summary

In this chapter, we studied the robustness of an interdependent system against cascading failures initiated by a random attack. This is done through a novel model where the constituent networks exhibit inherently different intra-dependency characteristics. In particular, inspired by many applications of interdependent cyber-physical systems (CPSs), our model consists of a flow network where failure of a node leads to flow redistribution and possible further failures due to *overloading* (i.e., the flow on a node exceeding its capacity), and a cyber-network where nodes need to be a part of the largest connected cluster to be functional. We derive relations for the dynamics of cascading failures, characterizing the mean fraction of surviving nodes from each network at every stage of the cascade. This leads to deriving the mean fraction of nodes that ultimately survive the cascade as a function of the initial attack size. Through simulations, we confirm our analysis and derive useful insights concerning the robustness of interdependent CPSs.

Part IV

Concluding Remarks and Future Work

Chapter 7

Concluding Remarks

This thesis studied the robustness of interdependent networks against cascading failures. As the critical infrastructures such as power systems or water distribution systems are becoming more interdependent, the threat of cascading failures that can lead to catastrophic system-wide damages raises great concern. Through carefully characterizing and modeling the inherent dependencies between and within different component networks, we provide a thorough analysis in understanding and mitigating the seemingly unexpected large-scale cascading failures. A main finding is that allocating the available redundancies uniformly across the system maximizes the robustness against random failures.

In particular, we considered the robustness of flow-carrying networks under random and targeted attacks, where we propose a global and equal flow redistribution model to capture the cascading failure dynamics. In the case of random attacks, we derive the final system size and critical attack size, and prove that the optimal robustness is reached when system redundancy is allocated uniformly. For targeted attacks, we propose the optimization problem of finding the best k lines to attack so as to minimize the number of alive lines at the steady-state, to reveal the worst-case attack vulnerability of the system. We also derive heuristic algorithms for the optimization problems proposed.

Besides flow-carrying networks, we consider interdependent networks composed of similar of inherently different component networks. For the first case, we consider an interdependent flow-carrying networks under random attacks. In interdependent flow-carrying networks, we study a model where the flow of a failed line is redistributed partially within the network that the failed

line belongs to, with the rest being shed to other coupled networks. Analyzing the cascading failures in this model, we show that interdependence has a multi-faceted impact on system robustness in that as the level of coupling increases, the chance for both networks to survive or collapse concurrently increases, whereas it becomes more difficult for each component network to survive on its own. The integrated cyber-physical systems (CPSs) is a typical example of interdependent networks composed of inherently different component networks (i.e., cyber networks and physical networks).To understand the robustness of the CPSs, we develop a novel interdependent system model to capture the inherently different failure cascade characteristics of each component network; i.e., the cyber and the physical networks are governed by different cascade rules to be able to function. We demonstrate the ability of our model to capture the unexpected nature of large-scale cascading failures in CPSs, and provide insights on improving system robustness by proposing optimal redundancy allocation schemes.

Chapter 8

Future Work

There are many open directions for future work. First of all, for flow-carrying networks, it would be interesting to analyze more complicated flow redistribution models based on network topology, rather than the equal redistribution model considered in most part of the thesis; e.g., the global-local redistribution model discussed in Section 6.5 with some preliminary simulation results. For targeted attacks considered in a flow-carrying network, one can further explore the complexity of the optimal k-attack problem (without a bound on the total load) since it's unknown. Also, with the results of Chapter 4 revealing *good* attack strategies, one might now seek optimal design strategies (e.g., in the form of load-capacity distributions) that lead to maximum robustness against such attacks. It might also be interesting to study *information cascades* in social networks [130–133] using the models considered here; the optimal attack problem studied here will then amount to *influence maximization* problem [134].

For interdependent networks, the simplistic one-to-one interdependence model used to build the interdependent relations can be replaced by more sophisticated and realistic dependency models. A good starting point would be to consider a model where every node is assigned m inter-links and can continue to function as long as at least one of its m support nodes in the other network is functional. It would be interesting to study the trade-off between the number of inter-links and the resulting improvements in overall system robustness; one might also consider a heterogeneous allocation of inter-links and study the optimal (in the sense of maximizing robustness) way to assign inter-links subject to certain constraints [22]. One can also extends our results to cases where the cyber-network is generated by richer models than

the configuration model. A good candidate would be random networks with clustering [135] that go beyond the degree distribution and specify also the number of triangles each node belongs to. Finally, it would be interesting to study the interdependent system robustness under targeted attacks [136] (where the set of nodes to be attacked is chosen carefully by an adversary) besides the case of random attacks considered in this thesis.

For the main finding in this thesis, which states that allocating the available redundancies uniformly across the system maximizes the robustness against random failures, one can further apply in real world system or platforms and evaluate effectiveness of the results on a more realistic setting. A possible case is the power grid, where one can test the result on a simulation platform for power grid analysis. A new and efficient platform is the SUGAR system [137–139], which is an equivalent split circuit formulation for power grid analysis. The system enables adaptation and application of techniques that were developed for *circuit simulation* to robustly analyze power grids, and unifies steady state, dynamics and transient analyses. Also, it assesses feasibility and solution of optimal power flow conditions in the simulation. The SUGAR system is specially powerful in analyzing cascading failures in power grid, in that the circuit-theoretic approach incorporates frequency deviations and implicit models for under-frequency/under-voltage load shedding, and it enables contingency analysis to calculate violations during the failure process. We tested the equal free-space allocation in some of the simple test cases, and in many cases it gives a better robustness when we adjust the line rating according to equal free-space allocation. More sophisticated experiments can be carried out in the platform with the uniform assign of system resource if one would continue this direction in the future. Besides adjusting line rating using equal free-space schemes, there are also many dynamic line rating schemes that one can explore in the future.

Bibliography

[1] Wikipedia contributors. 2019 venezuelan blackouts — Wikipedia, the free encyclopedia, 2019.

[2] Rod Walton. 13 years after: The northeast blackout of 2003 changed grid industry, still causes fear for future, Aug 2016.

[3] RD Christie. University of washington power systems test case archive (last accessed on 25 nov 2013)(1999). *URL http://www. ee. washington. edu/research/pstca*.

[4] NationalGrid. http://www2.nationalgrid.com/uk/industry-information/ future-of-energy/electricity-ten-year-statement/. Technical report, 2016.

[5] Albert-László Barabási and Réka Albert. Emergence of scaling in random networks. *Science*, 286:509–512, 1999.

[6] Wikipedia contributors. List of major power outages — Wikipedia, the free encyclopedia, 2019.

[7] A. Vespignani. Complex networks: The fragility of interdependency. *Nature*, 464:984–985, 2010.

[8] Dung T Nguyen, Yilin Shen, and My T Thai. Detecting critical nodes in interdependent power networks for vulnerability assessment. *IEEE Transactions on Smart Grid*, 4(1):151–159, 2013.

[9] Sergey V Buldyrev, Roni Parshani, Gerald Paul, H Eugene Stanley, and Shlomo Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025, 2010.

[10] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1):63–79, 01 2008.

[11]

[12] Sergey V Buldyrev, Nathaniel W Shere, and Gabriel A Cwilich. Interdependent networks with identical degrees of mutually dependent nodes. *Physical Review E*, 83(1):016112, 2011.

[13] Jianxi Gao, Sergey V Buldyrev, H Eugene Stanley, and Shlomo Havlin. Networks formed from interdependent networks. *Nature physics*, 8(1):40, 2012.

[14] Filippo Radicchi. Percolation in real interdependent networks. *arXiv preprint arXiv:1503.04655*, 2015.

[15] MA Di Muro, SV Buldyrev, HE Stanley, and LA Braunstein. Cascading failures in interdependent networks with finite functional components. *Physical Review E*, 94(4):042304, 2016.

[16] Ailing Huang, H Michael Zhang, Wei Guan, Yang Yang, and Gaoqin Zong. Cascading failures in weighted complex networks of transit systems based on coupled map lattices. *Mathematical Problems in Engineering*, 2015.

[17] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich. Interdependent networks with identical degrees of mutually dependent nodes. *Phys. Rev. E*, 83(016112), 2011.

[18] R. Parshani, S. V. Buldyrev, and S Havlin. Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition. *Phys. Rev. Lett.*, 105.

[19] X. Huang, J. Gao, S. Buldyrev, S. Havlin, and H. E. Stanley. Robustness of interdependent networks under targeted attack. *Phys. Rev. E*, 83(6), 2011.

[20] Di Zhou, Jianxi Gao, H. Eugene Stanley, and Shlomo Havlin. Percolation of partially interdependent scale-free networks. *Phys. Rev. E*, 87:052812, May 2013.

[21] Gaogao Dong, Jianxi Gao, Ruijin Du, Lixin Tian, H. Eugene Stanley, and Shlomo Havlin. Robustness of network of networks under targeted attack. *Phys. Rev. E*, 87:052804, May 2013.

[22] O. Yağan, D. Qian, J. Zhang, and D. Cochran. Optimal Allocation of Interconnecting Links in Cyber-Physical Systems: Interdependence, Cascading Failures and Robustness. *IEEE Transactions on Parallel and Distributed Systems*, 23(9):1708–1720, 2012.

[23] Yingrui Zhang and Osman Yağan. Optimizing the robustness of electrical power systems against cascading failures. *Scientific reports*, 6, 2016.

[24] E. M. Shahrivar and S. Sundaram. The game-theoretic formation of interconnections between networks. *IEEE Journal on Selected Areas in Communications*, 35(2):341–352, Feb 2017.

[25] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour. Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures. *IEEE Transactions on Communications*, 65(9):3847–3862, Sept 2017.

[26] Albert-László Barabási and Eric Bonabeau. Scale-free networks. *Scientific american*, 288(5):60–69, 2003.

[27] Albert-László Barabási. Scale-free networks: a decade and beyond. *science*, 325(5939):412–413, 2009.

[28] Romualdo Pastor-Satorras and Alessandro Vespignani. Epidemic spreading in scale-free networks. *Physical review letters*, 86(14):3200, 2001.

[29] Yang-Yu Liu, Jean-Jacques Slotine, and Albert-László Barabási. Controllability of complex networks. *nature*, 473(7346):167, 2011.

[30] Jesús Gómez-Gardeñes and Yamir Moreno. From scale-free to erdos-rényi networks. *Physical Review E*, 73(5):056124, 2006.

[31] Edward A Lee. Cyber physical systems: Design challenges. In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pages 363–369. IEEE, 2008.

[32] Réka Albert and Albert-László Barabási. Statistical mechanics of complex networks. *Reviews of modern physics*, 74(1):47, 2002.

[33] Albert-László Barabási. Linked: The new science of networks, 2003.

[34] Duncan J Watts. *Six degrees: The science of a connected age*. WW Norton & Company, 2004.

[35] Sergei N Dorogovtsev and José FF Mendes. *Evolution of networks: From biological nets to the Internet and WWW*. OUP Oxford, 2013.

[36] Mark EJ Newman. The structure and function of complex networks. *SIAM review*, 45(2):167–256, 2003.

[37] Mark Newman. *Networks: an introduction*. Oxford university press, 2010.

[38] Ryan Kinney, Paolo Crucitti, Reka Albert, and Vito Latora. Modeling cascading failures in the north american power grid. *The European Physical Journal B-Condensed Matter and Complex Systems*, 46(1):101–107, 2005.

[39] Christopher W Anderson, Joost R Santos, and Yacov Y Haimes. A risk-based input–output methodology for measuring the effects of the august 2003 northeast blackout. *Economic Systems Research*, 19(2):183–204, 2007.

[40] Wikipedia contributors. Northeast blackout of 2003 — Wikipedia, the free encyclopedia, 2019.

[41] Benjamin A Carreras, Vickie E Lynch, David E Newman, and Ian Dobson. Blackout mitigation assessment in power transmission systems. In *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, pages 10–pp. IEEE, 2003.

[42] Benjamin A Carreras, Vickie E Lynch, Ian Dobson, and David E Newman. Dynamics, criticality and self-organization in a model for blackouts in power transmission systems. In *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pages 9–pp. IEEE, 2002.

[43] Yuan Zhu, Kaan Ozbay, Hong Yang, Fan Zuo, and Di Sha. Modeling and simulation of cascading failures in transportation systems during hurricane evacuations. Technical report, 2019.

[44] Paolo Crucitti, Vito Latora, and Massimo Marchiori. Model for cascading failures in complex networks. *Physical Review E*, 69(4):045104, 2004.

[45] Xiuwen Fu, Haiqing Yao, and Yongsheng Yang. Exploring the invulnerability of wireless sensor networks against cascading failures. *Information Sciences*, 2019.

[46] Irena Vodenska and Alexander P Becker. Interdependence, vulnerability and contagion in financial and economic networks. In *New Perspectives and Challenges in Econophysics and Sociophysics*, pages 101–116. Springer, 2019.

[47] Kang Zhao, Zhiya Zuo, and Jennifer V Blackhurst. Modelling supply chain adaptation for disruptions: An empirically grounded complex adaptive systems approach. *Journal of Operations Management*, 65(2):190–212, 2019.

[48] Leonardo Duenas-Osorio and Srivishnu Mohan Vemuru. Cascading failures in complex infrastructure systems. *Structural safety*, 31(2):157–167, 2009.

[49] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406(6794):378–382, 2000.

[50] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts. Network robustness and fragility: Percolation on random graphs," network robustness and fragility: Percolation on random graphs. *Phys. Rev. Lett.*, 85(25):5468–5471, 2000.

[51] Reuven Cohen. Resilience of the internet to random breakdowns. *Phys. Rev. Lett.*, 85(21):4626–4628, 2000.

[52] Adilson E Motter, Takashi Nishikawa, and Ying-Cheng Lai. Range-based attack on links in scale-free networks: Are long-range links responsible for the small-world phenomenon? *Physical Review E*, 66(6):065103, 2002.

[53] Paolo Crucitti, Vito Latora, Massimo Marchiori, and Andrea Rapisarda. Efficiency of scale-free networks: error and attack tolerance. *Physica A: Statistical Mechanics and its Applications*, 320:622–642, 2003.

[54] Réka Albert, István Albert, and Gary L Nakarado. Structural vulnerability of the north american power grid. *Physical review E*, 69(2):025103, 2004.

[55] Yamir Moreno, JB Gómez, and AF Pacheco. Instability of scale-free networks under node-breaking avalanches. *EPL (Europhysics Letters)*, 58(4):630, 2002.

[56] Petter Holme and Beom Jun Kim. Vertex overload breakdown in evolving networks. *Physical Review E*, 65(6):066109, 2002.

[57] Adilson E Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. *Physical Review E*, 66(6):065102, 2002.

[58] Paolo Crucitti, Vito Latora, and Massimo Marchiori. A topological analysis of the italian electric power grid. *Physica A: Statistical mechanics and its applications*, 338(1-2):92–97, 2004.

[59] Adilson E. Motter and Ying-Cheng Lai. Cascade-based attacks on complex networks. *Phys. Rev. E*, 66:065102, Dec 2002.

[60] Liang Huang, Lei Yang, and Kongqing Yang. Geographical effects on cascading breakdowns of scale-free networks. *Physical Review E*, 73(3):036102, 2006.

[61] Jan Øystein Haavig Bakke, Alex Hansen, and János Kertész. Failures and avalanches in complex networks. *EPL (Europhysics Letters)*, 76(4):717, 2006.

[62] Luca Dall?Asta, Alain Barrat, Marc Barthélemy, and Alessandro Vespignani. Vulnerability of weighted networks. *Journal of Statistical Mechanics: Theory and Experiment*, 2006(04):P04006, 2006.

[63] Ingve Simonsen, Lubos Buzna, Karsten Peters, Stefan Bornholdt, and Dirk Helbing. Transient dynamics increasing network vulnerability to cascading failures. *Physical review letters*, 100(21):218701, 2008.

[64] M. E. J. Newman. Spread of epidemic disease on networks. *Phys. Rev. E*, 66(1), 2002.

[65] M. E. J. Newman, S. H. Strogatz, and D. J. Watts. Random graphs with arbitrary degree distributions and their applications. *Phys. Rev. E*, 64(2), 2001.

[66] Jia Shao, Sergey V Buldyrev, Shlomo Havlin, and H Eugene Stanley. Cascade of failures in coupled network systems with multiple support-dependence relations. *Physical Review E*, 83(3):036116, 2011.

[67] Christian M Schneider, Nuri Yazdani, Nuno AM Araújo, Shlomo Havlin, and Hans J Herrmann. Towards designing robust coupled networks. *Scientific reports*, 3:1969, 2013.

[68] Xuqing Huang, Jianxi Gao, Sergey V Buldyrev, Shlomo Havlin, and H Eugene Stanley. Robustness of interdependent networks under targeted attack. *Physical Review E*, 83(6):065101, 2011.

[69] Osman Yağan, Dajun Qian, Junshan Zhang, and Douglas Cochran. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *IEEE Transactions on Parallel and Distributed Systems*, 23(9):1708–1720, 2012.

[70] Enrico Zio and Giovanni Sansavini. Modeling interdependent network systems for identifying cascade-safe operating margins. *IEEE Transactions on Reliability*, 60(1):94–101, 2011.

[71] J. Shao, S. Buldyrev, S. Havlin, and H. E. Stanley. Cascade of failures in coupled network systems with multiple support-dependent relations. *Phys. Rev. E*, 83(036116), 2011.

[72] Charles D Brummitt, Raissa M D?Souza, and EA Leicht. Suppressing cascades of load in interdependent networks. *Proceedings of the National Academy of Sciences*, 109(12):E680–E689, 2012.

[73] Joshua J Romero. Blackouts illuminate india's power problems. *Spectrum, IEEE*, 49(10):11–12, 2012.

[74] Yong Tang, Guangquan Bu, and Jun Yi. Analysis and lessons of the blackout in indian power grid on july 30 and 31, 2012. In *Zhongguo Dianji Gongcheng Xuebao(Proceedings of the Chinese Society of Electrical Engineering)*, volume 32, pages 167–174. Chinese Society for Electrical Engineering, 2012.

[75] Dmitry N Kosterev, Carson W Taylor, William Mittelstadt, et al. Model validation for the august 10, 1996 wscc system outage. *Power Systems, IEEE Transactions on*, 14(3):967–979, 1999.

[76] Marian Anghel, Kenneth Werley, Adilson E Motter, et al. Stochastic model for power grid dynamics. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 113–113. IEEE, 2007.

[77] Paolo Crucitti, Vito Latora, and Massimo Marchiori. Model for cascading failures in complex networks. *Phys. Rev. E*, 69:045104, Apr 2004.

[78] Jian-Wei Wang and Li-Li Rong. Cascade-based attack vulnerability on the {US} power grid. *Safety Science*, 47(10):1332 – 1336, 2009.

[79] Sakshi Pahwa, Amelia Hodges, Caterina Scoglio, and Sean Wood. Topological analysis of the power grid and mitigation strategies against cascading failures. In *Systems Conference, 2010 4th Annual IEEE*, pages 272–276. IEEE, 2010.

[80] Osman Yağan. Robustness of power systems under a democratic-fiber-bundle-like model. *Phys. Rev. E*, 91:062811, Jun 2015.

[81] HE Daniels. The statistical theory of the strength of bundles of threads. i. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 183, pages 405–435. The Royal Society, 1945.

[82] Zhen Su, Lixiang Li, Haipeng Peng, Jürgen Kurths, Jinghua Xiao, and Yixian Yang. Robustness of interrelated traffic networks to cascading failures. *Scientific reports*, 4, 2014.

[83] Antonio Scala, Pier Giorgio De Sanctis Lucentini, Guido Caldarelli, and Gregorio D?Agostino. Cascades in interdependent flow networks. *Physica D: Nonlinear Phenomena*, 2015.

[84] Wen-Xu Wang and Guanrong Chen. Universal robustness characteristic of weighted networks against cascading failure. *Phys. Rev. E*, 77:026101, Feb 2008.

[85] Baharan Mirzasoleiman, Mahmoudreza Babaei, Mahdi Jalili, and MohammadAli Safari. Cascaded failures in weighted networks. *Physical Review E*, 84(4):046114, 2011.

[86] Andrey Bernstein, Daniel Bienstock, David Hay, Meric Uzunoglu, and Gil Zussman. Power grid vulnerability to geographically correlated failures?analysis and control implications. In *INFOCOM, 2014 Proceedings IEEE*, pages 2634–2642. IEEE, 2014.

[87] Evangelos Chatziafratis, Yingrui Zhang, and Osman Yağan. On the robustness of power systems: optimal load-capacity distributions and hardness of attacking. In *Information Theory and Applications Workshop (ITA), 2016*, Feb 2016.

[88] Osman Yağan. Robustness of power systems under a democratic-fiber-bundle-like model. *Phys. Rev. E*, 91:062811, Jun 2015.

[89] Richard Loulou and Eleftherios Michaelides. New greedy-like heuristics for the multidimensional 0-1 knapsack problem. *Operations Research*, 27(6):1101–1114, 1979.

[90] Y. Zhang and O. Yağan. Optimizing the robustness of electrical power systems against cascading failures. *Nature Scientific Reports*, 6:27625, 2016.

[91] Evangelos Chatziafratis, Yingrui Zhang, and Osman Yağan. On the robustness of power systems: optimal load-capacity distributions and hardness of attacking. In *Information Theory and Applications Workshop (ITA)*, 2016.

[92] Shizuo Senju and Yoshiaki Toyoda. An approach to linear programming with 0-1 variables. *Management Science*, pages B196–B207, 1968.

[93] Yoshiaki Toyoda. A simplified algorithm for obtaining approximate solutions to zero-one programming problems. *Management Science*, 21(12):1417–1427, 1975.

[94] Wei Li, Amir Bashan, Sergey V Buldyrev, H Eugene Stanley, and Shlomo Havlin. Cascading failures in interdependent lattice networks: The critical role of the length of dependency links. *Physical review letters*, 108(22):228702, 2012.

[95] Jianxi Gao, Sergey V Buldyrev, Shlomo Havlin, and H Eugene Stanley. Robustness of a network of networks. *Physical Review Letters*, 107(19):195701, 2011.

[96] Steven M Rinaldi. Modeling and simulating critical infrastructures and their interdependencies. In *System sciences, 2004. Proceedings of the 37th annual Hawaii international conference on*, pages 8–pp. IEEE, 2004.

[97] Ginestra Bianconi and Sergey N. Dorogovtsev. Multiple percolation transitions in a configuration model of a network of networks. *Phys. Rev. E*, 89:062814, Jun 2014.

[98] D. Qian, O. Yağan, L. Yang, and J. Zhang. Diffusion of real-time information in social-physical networks. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 2072–2077, Dec 2012.

[99] Yong Zhuang and Osman Yağan. Information propagation in clustered multilayer networks. *IEEE Transactions on Network Science and Engineering*, 3(4):211–224, 2016.

[100] Osman Yağan and Virgil Gligor. Analysis of complex contagions in random multiplex networks. *Physical Review E*, 86(3):036103, 2012.

[101] O. Yağan, D. Qian, J. Zhang, and D. Cochran. Conjoining speeds up information diffusion in overlaying social-physical networks. *IEEE Journal on Selected Areas in Communications*, 31(6):1038–1048, June 2013.

[102] Yong Zhuang, Alex Arenas, and Osman Yağan. Clustering determines the dynamics of complex contagions in multiplex networks. *Phys. Rev. E*, 95:012312, Jan 2017.

[103] Seung-Woo Son, Golnoosh Bizhani, Claire Christensen, Peter Grassberger, and Maya Paczuski. Percolation theory on interdependent networks based on epidemic spreading. *EPL (Europhysics Letters)*, 97(1):16006, 2012.

[104] Byungjoon Min, Su Do Yi, Kyu-Min Lee, and K-I Goh. Network robustness of multiplex networks with interlayer degree correlations. *Physical Review E*, 89(4):042811, 2014.

[105] Kyu-Min Lee, Charles D Brummitt, and K-I Goh. Threshold cascades with response heterogeneity in multiplex networks. *Physical Review E*, 90(6):062816, 2014.

[106] Chong Wu, Shenggong Ji, Rui Zhang, Liujun Chen, Jiawei Chen, Xiaobin Li, and Yanqing Hu. Multiple hybrid phase transition: Bootstrap percolation on complex networks with communities. *EPL (Europhysics Letters)*, 107(4):48001, 2014.

[107] Alessandro Vespignani. Complex networks: The fragility of interdependency. *Nature*, 464(7291):984–985, 2010.

[108] Ravá da Silveira. An introduction to breakdown phenomena in disordered systems. *American Journal of Physics*, 67(12):1177–1188, 1999.

[109] Y Moreno, AM Correig, JB Gómez, and AF Pacheco. A model for complex aftershock sequences. *Journal of Geophysical Research: Solid Earth*, 106(B4):6609–6619, 2001.

[110] Donald L Turcotte and Margaret T Glasscoe. A damage model for the continuum rheology of the upper continental crust. *Tectonophysics*, 383(1):71–80, 2004.

[111] Yingrui. Zhang and Osman Yağan. Optimizing the robustness of electrical power systems against cascading failures. *Scientific Reports*, 6:27625 EP, 2016.

[112] Srutarshi Pradhan, Alex Hansen, and Bikas K Chakrabarti. Failure processes in elastic fiber bundles. *Reviews of modern physics*, 82(1):499, 2010.

[113] Helmut Elsinger, Alfred Lehar, and Martin Summer. Risk assessment for banking systems. *Management science*, 52(9):1301–1314, 2006.

[114] Roni Parshani, Sergey V Buldyrev, and Shlomo Havlin. Critical effect of dependency groups on the function of networks. *Proceedings of the National Academy of Sciences*, 108(3):1007–1010, 2011.

[115] Antonio Scala, Pier Giorgio De Sanctis Lucentini, Guido Caldarelli, and Gregorio D'Agostino. Cascades in interdependent flow networks. *Physica D: Nonlinear Phenomena*, 323:35–39, 2016.

[116] Wen-Xu Wang and Guanrong Chen. Universal robustness characteristic of weighted networks against cascading failure. *Physical Review E*, 77(2):026101, 2008.

[117] Baharan Mirzasoleiman, Mahmoudreza Babaei, Mahdi Jalili, and MohammadAli Safari. Cascaded failures in weighted networks. *Physical Review E*, 84(4):046114, 2011.

[118] Raissa M D'souza. Curtailing cascading failures. *Science*, 358(6365):860–861, 2017.

[119] Ebrahim Moradi Shahrivar, Mohammad Pirani, and Shreyas Sundaram. Spectral and structural properties of random interdependent networks. *Automatica*, 83:234–242, 2017.

[120] Yingrui Zhang, Alex Arenas, and Osman Yağan. Cascading failures in interdependent systems under a flow redistribution model. *Phys. Rev. E*, 97:022307, Feb 2018.

[121] Jørgen Vitting Andersen, Didier Sornette, and Kwan-tai Leung. Tricritical behavior in rupture induced by disorder. *Physical Review Letters*, 78(11):2140, 1997.

[122] Sakshi Pahwa, Caterina Scoglio, and Antonio Scala. Abruptness of cascade failures in power grids. *Scientific reports*, 4, 2014.

[123] M. Molloy and B. Reed. A critical point for random graphs with a given degree sequence. *Random Structures and Algorithms*, 6:161–179, 1995.

[124] B. Bollobás. *Random Graphs*. Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge (UK), 2001.

[125] Paul Erdös and Alfréd Rényi. On random graphs, i. *Publicationes Mathematicae (Debrecen)*, 6:290–297, 1959.

[126] Paul Erdös and Alfréd Rényi. On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci*, 5(17-61):43, 1960.

[127] Béla Bollobás. Random graphs. In *Modern graph theory*, pages 215–252. Springer, 1998.

[128] Aaron Clauset, Cosma Rohilla Shalizi, and M. E. J. Newman. Power-law distributions in empirical data. *SIAM Rev.*, 51(4):661–703, November 2009.

[129] Réka Albert, Hawoong Jeong, and Albert-László Barabási. Internet: Diameter of the world-wide web. *nature*, 401(6749):130, 1999.

[130] D. J. Watts. A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences*, 99:5766–5771, 2002.

[131] Osman Yağan and Virgil Gligor. Analysis of complex contagions in random multiplex networks. *Physical Review E*, 86(3):036103, 2012.

[132] Osman Yağan, Dajun Qian, Junshan Zhang, and Douglas Cochran. Information diffusion in overlaying social-physical networks. In *2012 46th Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE, 2012.

[133] O. Yağan, D. Qian, J. Zhang, and D. Cochran. Conjoining speeds up information diffusion in overlaying social-physical networks. *arXiv:1112.4002v2 [cs.SI]*, 2011.

[134] David Kempe, Jon Kleinberg, and Éva Tardos. Maximizing the spread of influence through a social network. In *Proc. of ACM SIGKDD Conference*, pages 137–146, 2003.

[135] Mark EJ Newman. Random graphs with clustering. *Physical review letters*, 103(5):058701, 2009.

[136] Talha Cihad Gulcu, Vaggos Chatziafratis, Yingrui Zhang, and Osman Yağan. Attack vulnerability of power systems under an equal load redistribution model. *IEEE/ACM Transactions on Networking*, 26(3):1306–1319, 2018.

[137] Amritanshu Pandey, Aayushya Agarwal, Marko Jereminov, Martin R Wagner, David M Bromberg, and Larry Pileggi. Robust sequential steady-state analysis of cascading outages. *arXiv preprint arXiv:1904.11125*, 2019.

[138] Amritanshu Pandey. *Robust Steady-State Analysis of the Power Grid using an Equivalent Circuit Formulation with Circuit Simulation Methods*. PhD thesis, Carnegie Mellon University, 2019.

[139] Amritanshu Pandey, Marko Jereminov, Martin R Wagner, David M Bromberg, Gabriela Hug, and Larry Pileggi. Robust power flow and three-phase power flow analyses. *IEEE Transactions on Power Systems*, 34(1):616–626, 2019.