Robustness of Interdependent Cyber-Physical Systems Against Cascading Failures

Yingrui Zhang, *Student Member, IEEE*, and Osman Yağan, *Senior Member, IEEE*

***Abstract*—Integrated cyber-physical systems, such as the smart-grid, are increasingly becoming the underpinning technology for major industries. A major concern regarding such systems are the seemingly unexpected large scale failures, which are often attributed to a small initial shock getting escalated due to intricate dependencies within and across the individual (e.g., cyber and physical) counterparts of the system. In this paper, we develop a novel interdependent system model to capture this phenomenon, also known as cascading failures. Our framework consists of two networks that have inherently different characteristics governing their intradependence: first, 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, second, 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). Furthermore, it is assumed that these two networks are *interdependent*. For simplicity, we consider a one-to-one interdependence 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.). Analytic results are supported through an extensive numerical study. 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.**

***Index Terms*—Analytical models, complex systems, cyber-physical systems, graphical models, Robustness.**

I. Introduction

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 [35] 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 [6]. For example, it was shown in [30] that the electrical blackout that affected much of Italy on September 28, 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. Toward 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 [6], [8], [13], [19], [29], [43], very few consider engineering aspects of interdependent networks and very little is known as to how such systems can be designed to have maximum robustness under certain design constraints; see [9], [33], [39], [41] for rare exceptions. The current literature

Manuscript received July 20, 2018; revised July 23, 2018 and March 25, 2019; accepted May 4, 2019. Date of publication May 21, 2019; date of current version January 28, 2020. This work was supported by the National Science Foundation under Grant CCF #1422165. This paper was presented in part at the 57th IEEE International Conference on Decision and Control, Miami Beach, FL, December 2018 [42]. Recommended by Associate Editor R. M. Jungers. *(Corresponding author: Osman Yagan.)*

The authors are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: yingruiz@andrew.cmu.edu; oyagan@ece.cmu.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2019.2918120

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 CPSs.

In this paper, 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 intradependence models for each constituent network as well as an interdependence model describing the spread of failures *across* networks; see Section II-A 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 [14].

Our interdependent system model consists of 1) a cyber-network where a node is assumed to be functional as long as it belongs to the largest connected (i.e., giant) component; and 2) 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). For simplicity, we consider a one-to-one interdependence model where every node in the cyber-network is dependent upon and supports a single node in the physical network, and vice versa. Thus, a node in the cyber-network (resp. physical network) will continue to function if and only if its support in the physical network (resp. cyber-network) is functional *and* it belongs to the largest connected subgraph of the cyber-network (resp. its capacity is larger than its current flow); see Section II for a detailed description of the system model.

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 [6], [39] 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 [11], [20], [22], [37] 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 [3] 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 paper 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 toward flow-redistribution models, *and* toward 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 paper 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.

The rest of this paper is organized as follows. In Section II, we present our interdependent system model in details, starting with the distinction between intradependence and interdependence. In Section III, we present the main result of this paper, which allows computing the fraction of surviving nodes at each step of cascading failures initiated by a random attack. Here, we also provide an outline of the proof, while full proof is given in the Appendix. In Section IV, we present numerical results demonstrating the accuracy of our analysis in the finite node regime. This paper is concluded in Section VI with several suggestions for future work.

II. System Model

A. Intradependence Versus Interdependence

Our modeling framework is motivated from the inherent dependencies that exist in many real-world systems including CPSs. Namely, we characterize how component failures propagate and cascade, both within the cyber or the physical parts of the system (due to "intradependence"), as well as across them due to "interdependence." 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. For ease of exposition, we consider two subsystems, 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 intradependencies. 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 interdependence 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 interdependencies in the cascade of failures, consider an *asynchronous* failure update model, where the effect of intradependencies and interdependencies are considered in two separate batches, following one another. See Fig. 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 cannot heal once failed.

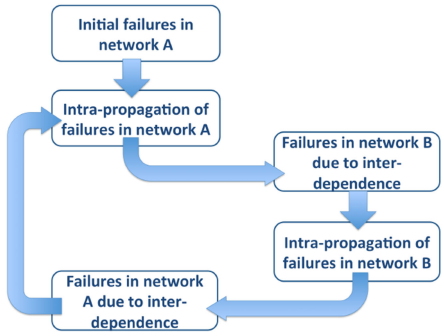

Fig. 1. Illustration of failure propagation model in an interdependent system.

B. Model

Despite the vast literature on interdependent networks [6], [32], [39], [40], there has been little (if any) attempt to characterize the robustness of interdependent systems where the constituent networks have different intradependence 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 interdependent system model that consists of two networks with different characteristics governing their intradependence: 1) 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 2) 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 intradependence; most existing works are focused on the interdependence between two physical networks (that obey a flow-redistribution-based model) [31], or two cyber-networks (that obey a giant-component-based intrafailure model) [6].

Intradependence 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

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

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

intradependence 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 [2], [12], and has been recently used by Pahwa *et al.* [28] in the context of power systems; see also [26], [38], [41]. 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 [11], [36], e.g., it was suggested by Pahwa *et al.* [27] that equal flow redistribution is a reasonable assumption especially under the dc power flow model. In Section V, 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.

Intradependence in network B. Let network B represent a cyber-network (e.g., communication) 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 extensively analyzed in the case of *single* networks [3], [23], [25]. The focus has recently been shifted toward *interdependent* networks with the work of Buldyrev *et al.* [6], where robustness of two interdependent networks, both operating under the giant-component-based intradependence rule, were 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 intradependencies.

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 [5], [21], [25] 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.

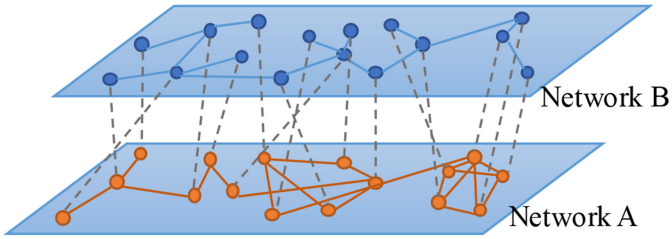

Fig. 2. System model illustration for the CPSs, where network A can be the physical grid, and network B can be the communication network that sends control signals. The interdependence across the two networks are realized through random one-to-one support links shown by dashed lines. Our analysis of 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).

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 Fig. 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 [6]; 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 Fig. 1, we assume an asynchronous cascade model, where intrapropagation and interpropagation 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 1) its current flow at time t is less than its capacity; *and* 2) 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 1) it belongs to largest connected component of B at time t; and 2) 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 ids 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

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

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 $0 \le p \le 1$. This is followed in Section IV 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 CPS can be improved by careful allocation of available resources (e.g., node capacities and degrees).

III. Main Result

Our main result is presented in the following. 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 $A_1 \supset A_3 \supset \cdots \supset A_{2i+1}$ and $B_2 \supset B_4 \supset \cdots \supset B_{2i}$ 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.,

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

We define f_{B_i} similarly as

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

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

Theorem 3.1: Consider an interdependent system as described in Section II, 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 $\mathbb{P}$ [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 $i = 0, 1, \ldots$

TABLE I
Key Notation in the Analysis of Cascading Failures

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 $f_{B_{2i+2}}$

The notation used in Theorem 3.1 is summarized in Table I. 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 (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) always holds with $u = 0$. Thus, if at any stage i, there is no $u > 0$ satisfying the equality in (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.

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 the Appendix. In [41], 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 [41] are incorporated in the recursions above through expression (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 the Appendix, given that the intrafailure 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 $t = 2i-1$, $i = 1, 2, \ldots$, 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 interdependence 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 the 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 (2)–(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 $t = 2i + 2, i = 0, 1, 2, \ldots$ 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 [6]. 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 (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 [6], [17], [23], [25], [34]. The formulas that give the network size $f_{B_{2i+2}}$ at each time stage $i = 0, 1, \ldots$ are presented at (6) and (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 (2) and (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 (2)–(7) shown at the bottom of this page.

IV. 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: 1) uniform, 2) Pareto, and 3) 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 [27]. 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.

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

$$\begin{aligned} Q_{2i+1} &= Q_{2i-1} + \min\left\{ x \in (0,\infty] : \frac{\mathbb{P}\left[S > Q_{2i-1} + x\right]}{\mathbb{P}\left[S > Q_{2i-1}\right]}(x + Q_{2i-1} + \mathbb{E}\left[L | S > x + Q_{2i-1}\right]) \right. \\ &\geq \left. \frac{Q_{2i-1} + \mathbb{E}\left[L | S > Q_{2i-1}\right]}{p_{A_{2i+1}}} \right\} \end{aligned} \tag{3}$$

$$f_{A_{2i+1}} = f_{A_{2i-1}} \cdot p_{A_{2i+1}} \cdot \mathbb{P}\left[S > Q_{2i+1} | S > Q_{2i-1}\right] \tag{4}$$

$$p_{B_{2i+2}} = p_{B_{2i}} \frac{f_{A_{2i+1}}}{f_{B_{2i}}} \tag{5}$$

$$u_{2i+2} = \max\left\{ u \in [0,1] : u = 1 - \sum_{k=0}^{\infty} \frac{k d_k}{\langle d \rangle} (1 - u \cdot p_{B_{2i+2}})^{k-1} \right\} \tag{6}$$

$$f_{B_{2i+2}} = p_{B_{2i+2}} \left(1 - \sum_{k=0}^{\infty} d_k \left(1 - u_{2i+2} \cdot p_{B_{2i+2}}\right)^k \right). \tag{7}$$

The corresponding probability density functions are defined in the following for a generic random variable L.

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

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

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

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

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.

3) Weibull distribution: $L \sim \mathrm{Weibull}(L_{\min}, \lambda, k)$. With $\lambda, k, L_{\min} > 0$, the density is given by

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

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

As explained in Section II-B, 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 in the following.

1) Erdős–Rényi (ER) network model [4], [15], [16]. This corresponds to having the degree distribution d_k follow a Binomial distribution, i.e., $d_k \sim \mathrm{Binomial}(N-1; \frac{\langle d\rangle}{N-1})$; as before $\langle d\rangle$ gives the mean node degree.

2) The scale-free (SF) network model [3]. We consider the case where the degree distribution $\{d_k\}_{k=0}^\infty$ is a *power-law* with *exponential cutoff*, which was observed [10] in many real networks including the Internet, i.e., we have

$$d_k = \begin{cases} 0 & \text{if } k = 0 \\ \frac{1}{\mathrm{Li}_\gamma\left(e^{-1/\Gamma}\right)} k^{-\gamma} e^{-k/\Gamma} & \text{if } k = 1, 2, \ldots \end{cases} \quad (8)$$

where γ is the power exponent, Γ is the cutoff 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.

A. Fiber Network Coupled With the ER Network

The ER 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 $\langle d\rangle$.

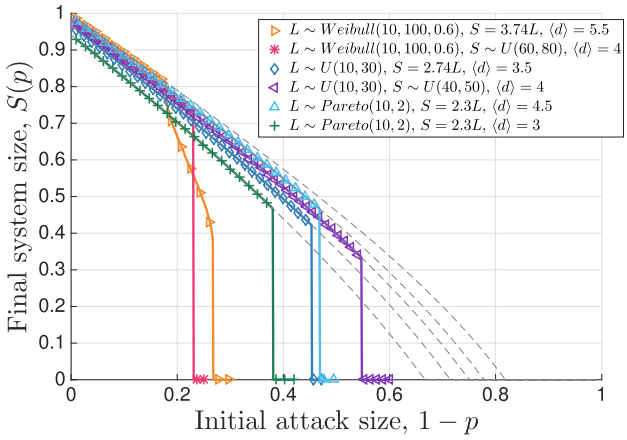

Fig. 3. Final system size under different network settings, including different load–"free space" distributions in the physical network and different mean degree in the cyber-network modeled by an ER network. Analytic results are represented by lines, whereas simulation results are represented by symbols (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.

First, we confirm our main result presented in Section III 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 Fig. 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 (2)–(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 Fig. 3 are as follows. From left to right, we have the following.

1) In network A (the physical network), L is Weibull with $L_{\min} = 10, \lambda = 100, k = 0.6$, and $S = \alpha L$ with $\alpha = 3.74$; in network B (the cyber-network) the mean degree $\langle d\rangle = 5.5$.
2) In network A, L is Weibull with $L_{\min} = 10, \lambda = 100, k = 0.6$, and S is uniform over [60, 80]; in network B $\langle d\rangle = 4$.
3) L is uniform over [10,30] and $S = \alpha L$ with $\alpha = 2.74$; in network B $\langle d\rangle = 3.5$.

[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.

4) L is uniform over $[10, 30]$ and S is uniform over $[40, 50]$; $\langle d \rangle = 4$.
5) L is Pareto with $L_{\min} = 10, b = 2, S = \alpha L$ with $\alpha = 2.3$; $\langle d \rangle = 4.5$.
6) L is Pareto with $L_{\min} = 10, b = 2, S = \alpha L$ with $\alpha = 2.3$; $\langle d \rangle = 3$.

In Fig. 3, gray dashed lines correspond to the case where a single cyber-network (with the same parameters used in Fig. 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 Fig. 3 show how different load–"free space" distributions in network A as well 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 Fig. 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 Fig. 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

[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.

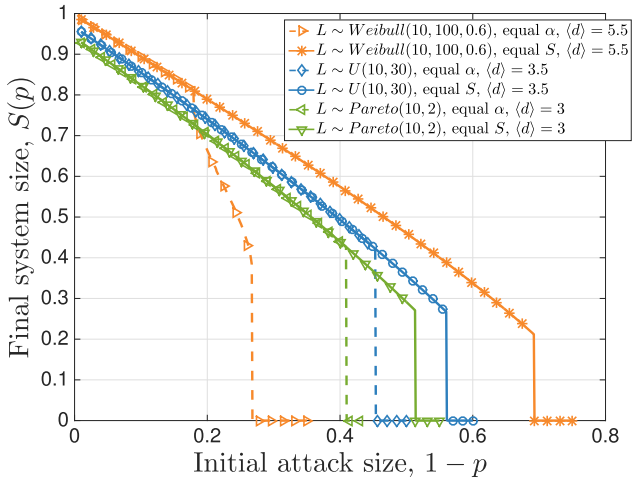

Fig. 4. Final system size under equal free space (solid lines with symbols) or equal tolerance factor (dashed lines with symbols) when network B is a ER graph with fixed mean degree. The symbols are empirical results over 100 independent runs on network size $N = 10^5$, and lines (dashed or solid) represent 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.

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-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 [11], [20], [22], [37] used for the entire network. We already showed in [41] that 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 Fig. 4, show that the above-mentioned 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 Fig. 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., $1-p^\star=0.7$ versus $1-p^\star=0.28$.

B. Fiber Network Coupled With the 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, SF networks model were shown [1] 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 [10], power-law distributions with exponential cutoff also ensure that all moments of the node degree are *finite*, which helps certain convergences take place faster (i.e., with smaller N).

In Fig. 5, we verify our analytic results when network B (cyber-network) has a degree distribution in the form of a power-law with exponential cutoff; this is denoted by $\mathrm{SF}(\gamma,\Gamma)$, where γ is the power exponent and Γ is the cutoff parameter given at (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 versus SF model) affect the system robustness. With the discussion from Section IV-A in mind, we consider the widely 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 [41] 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.

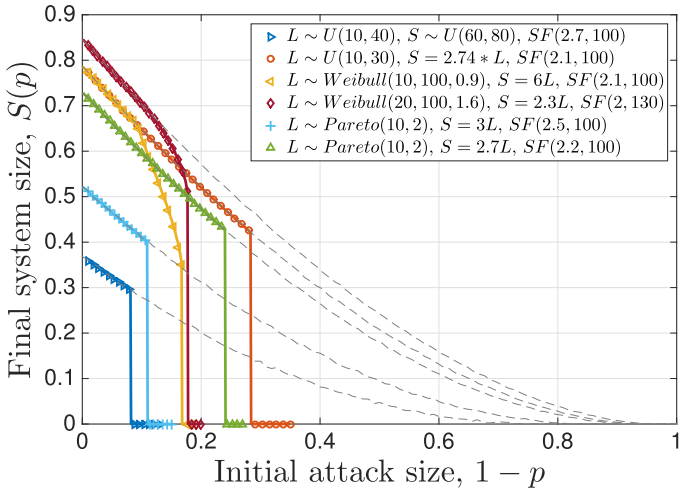

Fig. 5. Final system size under different network settings, including different load–"free space" distributions in the physical network and different exponent in the SF cyber-network. Analytic results are represented by lines, whereas simulation results are represented by symbols (averaged over 100 independent 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.

The results are shown in Fig. 6. We can see that no matter how the initial load is distributed, i.e., whether it is 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 the 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 Fig. 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 [3] 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

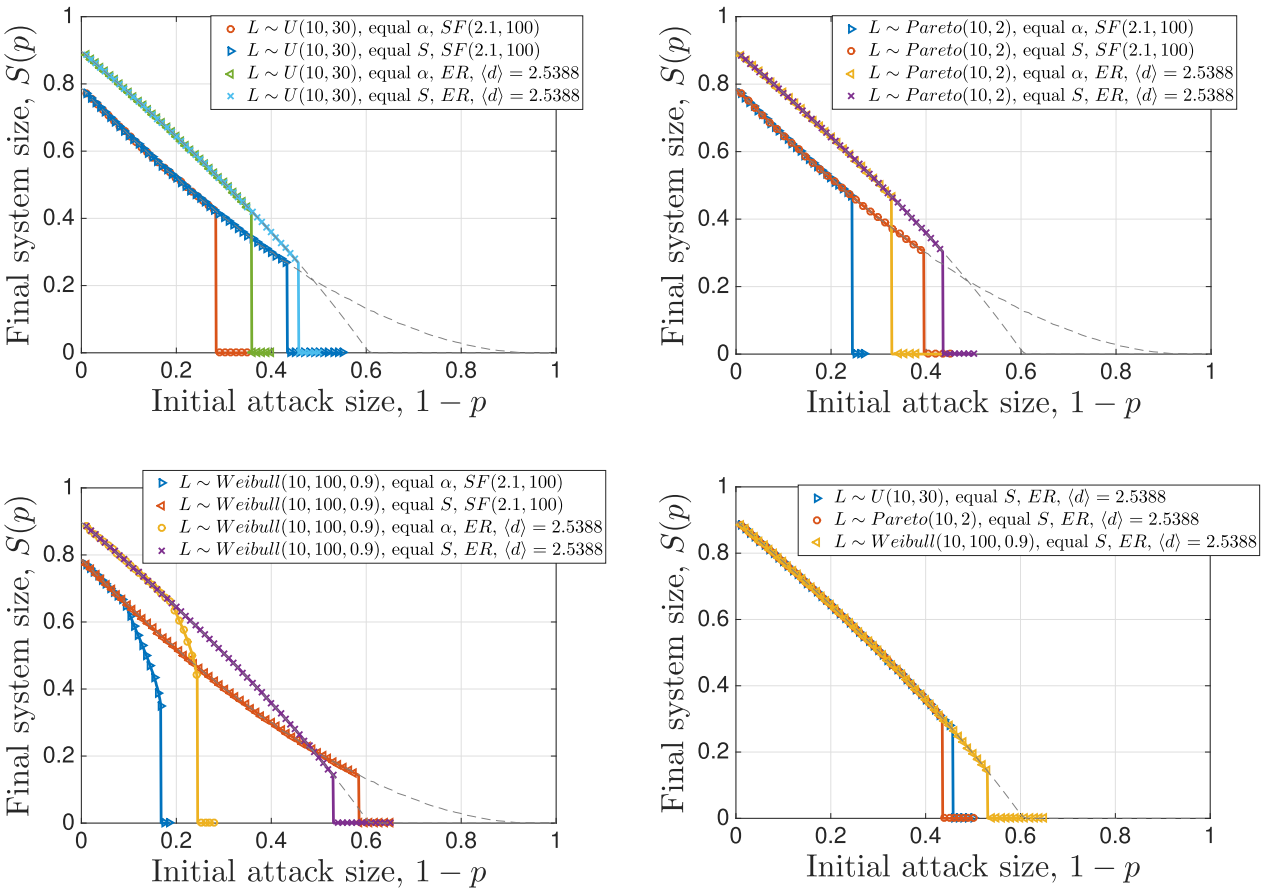

Fig. 6. Comparison of final system size when equal tolerance factor (equal α) and equal free space (equal S) schemes are used. The mean value of free space is kept the same, as well as the mean degree in SF and ER networks. In all cases, equal S outperform the widely used equal α scheme. The effect of 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 [3] 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).

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 Fig. 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 cannot 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 Fig. 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 the case when it is SF. However, if a robust physical network with *large* critical attack size is made interdependent with a cyber-network, then the CPS is more robust when the cyber-network is SF.

V. 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,

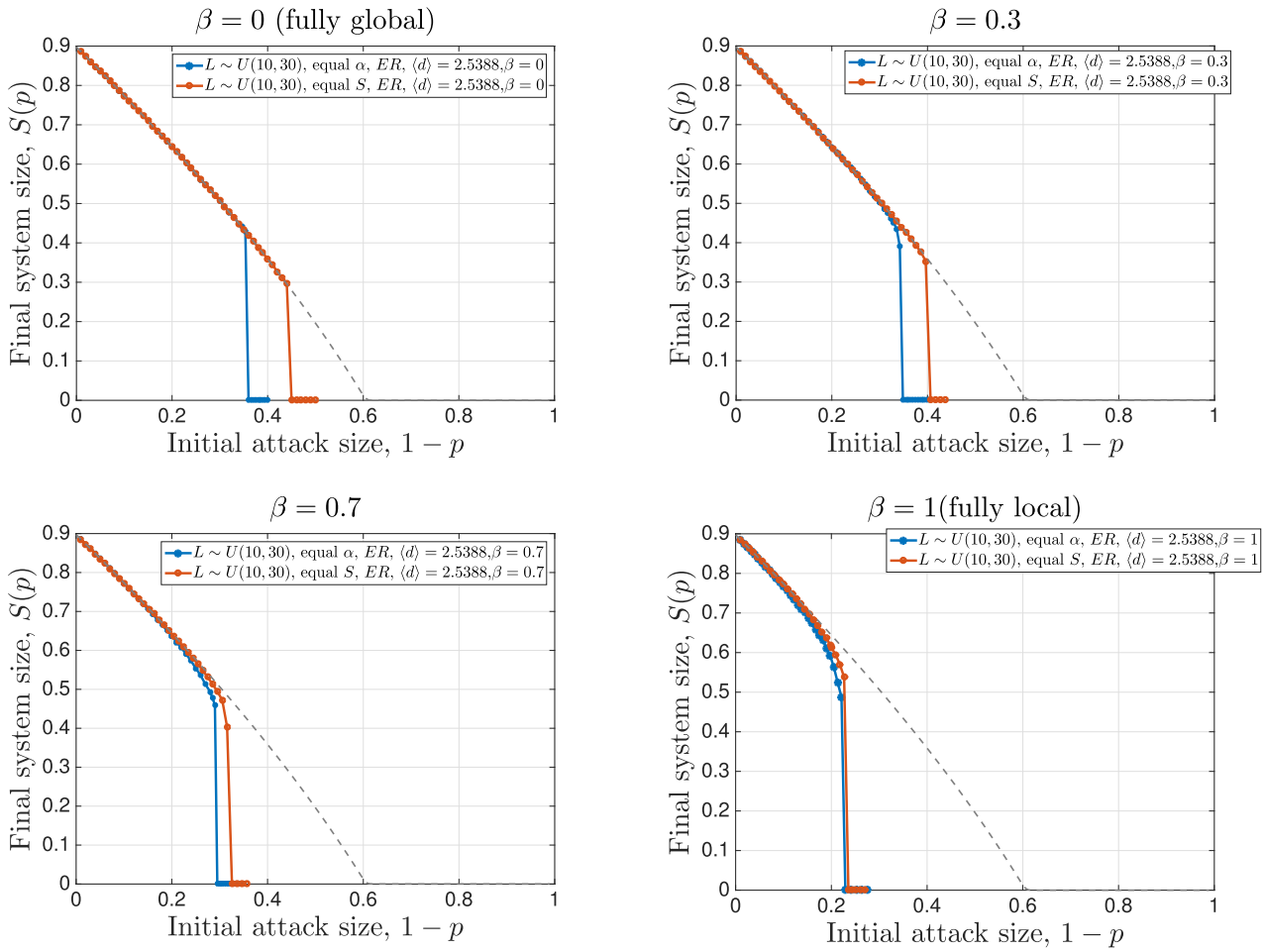

Fig. 7. Physical network adopts the global-local redistribution rule under ER topology, with β denoting the fraction of flow redistributed locally. The gray dashed line represents the case when a single ER graph is randomly attacked. In all cases, we see that equal-S allocation outperforms the equal-α allocation, meaning that the qualitative behavior of the robustness remains unchanged under different β values.

at least in part, according to this topology. To this end, we consider *global-local combined* redistribution model [40], where β fraction of load will go to the neighbors of a failed node, and $1 - \beta$ fraction of load will go to all remaining nodes in the network. The intradependence in the cyber-network and the interdependence model between the two networks remain the same. With this approach, we recover the model analyzed in our paper when $\beta = 0$, while setting $\beta = 1$ leads to a fully topology based redistribution model in the physical network.

In Fig. 7, we present simulation results showing the robustness of an interdependent CPS under different β 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 Fig. 7 that as β changes from 0 to 1, i.e., when the physical network gradually changes from a fully global redistribution model ($\beta = 0$) to a fully local redistribution model ($\beta = 1$), the robustness of the whole system decreases. However, the qualitative behavior of the robustness remains unchanged under different β 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 $\beta = 0$) is able to capture well the qualitative behavior of final system size for all β values.

VI. Conclusion

We have 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 intradependence characteristics. In particular, inspired by many applications of interdependent 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.

There are many open directions for future work. First of all, the simplistic one-to-one interdependence model used here can be replaced by more sophisticated and realistic dependence models. A good starting point would be to consider a model where every node is assigned k interlinks and can continue to function as long as at least one of its k support nodes in the other network is functional. It would be interesting to study the tradeoff between the number of interlinks and the resulting improvements in overall system robustness; one might also consider a heterogeneous allocation of interlinks and study the optimal (in the sense of maximizing robustness) way to assign interlinks subject to certain constraints [39]. It would also be interesting the analyze more complicated flow redistribution models based on network topology, rather than the equal redistribution model considered here, e.g., the global-local redistribution model discussed in Section V. Our results can also be extended to cases where the cyber-network is generated by richer models than the configuration model. A good candidate would be random networks with clustering [24] 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 system robustness under targeted attacks [18] (where the set of nodes to be attacked is chosen carefully by an adversary) rather than the case of random attacks considered in this paper.

APPENDIX
PROOF OF THE MAIN RESULT

We now prove the main result of this paper, i.e., Theorem 3.1. This entails 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 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 $A_1 \supset A_3 \supset \cdots \supset A_{2i+1}$ and $B_2 \supset B_4 \supset \cdots \supset B_{2i}$ 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.,

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

We define f_{B_i} similarly as

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

A. Computing the Functional Component in the Physical Network

First, we consider the intrafailures within the physical network A and derive f_{A_i} for $i = 1, 3, \ldots$. Initially, $1 - p_{A_1}$ fraction of nodes are attacked (or, failed) randomly in network A, where $p_{A_1} \in [0, 1]$. The flow in the failed nodes will get redistributed (equally) to all remaining nodes that are not attacked. Each such node will now have an increased load on them. If the extra load received is greater than the free space on a node (equivalently, if the current load is greater than their capacity), it will fail resulting in another round of redistribution, and so on and so forth.

In our previous work [41], we analyzed the cascading failures in a single flow network and obtained results that allows computing 1) the fraction of nodes that will survive at the steady state of cascades; and 2) the extra load that each surviving line will be carrying, once the *steady state* is reached. Here, this result, presented in the following as Theorem A.1 for convenience, will be used in calculating the outcome of each round of intrafailures in network A.

Theorem A.1 (see[41]): Consider a flow network of N nodes as described in Section II-B. Let L and S denote generic random variables following the same distribution (i.e., $p_{LS}(x, y)$) with initial loads $L_1, \ldots, L_N$, and free spaces $S_1, \ldots, S_N$, respectively. Let $n_\infty(p)$ be the *mean* fraction of nodes that are still functioning at the steady of cascading failures initiated by a random attack on $(1 - p)$-fraction of the nodes. Then, we have

$$n_\infty(p) = p\mathbb{P}\left[S > x^\star\right] \tag{A.1}$$

with $x^\star$ denoting the *extra load carried by each node that survives at the steady state* and is given by

$$x^\star = \min\Bigg\{x \in (0, \infty] : \mathbb{P}\left[S > x\right](x + \mathbb{E}\left[L | S > x\right]) \geq \frac{\mathbb{E}\left[L\right]}{p}\Bigg\}. \tag{A.2}$$

In words, this result states that when $(1 - p)$-fraction of nodes fail randomly in a flow network where the initial load–"free-space" distribution is given by p_{LS}, the cascading failures (caused by recursive load redistribution) will stop with $p\mathbb{P}[S > x^\star]$-fraction of nodes surviving, and the load–"free-space" distribution of surviving nodes will be updated as

$$L^{(\cdot)} \sim L + x^\star | S > x^\star \tag{A.3}$$

$$S^{(\cdot)} \sim S - x^\star | S > x^\star \tag{A.4}$$

where $x^\star$ is as defined in (A.2). These observations as well as (A.1) follow immediately from the fact that $x^\star$ gives the amount of extra load each surviving node carries at the steady state; see [41] for a detailed explanation of this fact. For example, (A.1) is seen easily as the probability that a node is *not* in the initial set of $(1 - p)$-fraction of failed nodes, *and* has more free space than the $x^\star$ amount of load it receives through redistribution from nodes that failed at any step of the cascade. Also, given that a node survives this cascade of failures, the probability distribution of its load–"free-space" values need to be updated via conditioning on the fact that its free space satisfies $S > x^\star$.

Noting also that each surviving node will now carry $x^\star$ amount of *extra* load in addition to its initial load, and will have $x^\star$ amount of *less* free space than it started with, we obtain (A.3) and (A.4).

In the forthcoming discussion, we will repeatedly use the fact that the set of nodes that survive at the steady state still form a flow network as described in Section II-B, with its fractional size reduced to $p\mathbb{P}[S > x^\star]$ and its load–"free-space" distribution updated via (A.3) and (A.4). For the interdependent network model under consideration, the intrafailures in network A will be followed by failures in network B first due to interdependence, and then due to intradependence in B, with the latter possibly triggering further failures in A (e.g., see Fig. 1). For instance, for any stage $i = 0, 1, \ldots$, let us assume that the intrafailures in network A has just resulted in A_{2i-1}. This will be followed by the aforementioned failures in B leading to B_{2i}. Since intrafailure 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_{2i-1}; in fact, it will be equivalent to a random attack targeting $1 - |B_{2i}|/|A_{2i-1}|$ -fraction of the nodes. The discussion mentioned above shows that we can compute the outcome of this random attack again from Theorem A.1 and obtain the size of A_{2i+1}, and so on.

With these in mind, we now start by computing f_{A_1}, which gives the resulting size of network A after a random attack to $1 - p_{A_1}$-fraction of nodes, i.e., f_{A_1} gives the fraction of nodes in A_1. Using Theorem A.1, we immediately get

$$f_{A_1} = p_{A_1}\mathbb{P}\left[S > x_1^\star\right] \tag{A.5}$$

where $x_1^\star$ is given from

$$x_1^\star = \min\Bigg\{x \in (0,\infty] : \mathbb{P}\left[S > x\right](x + \mathbb{E}\left[L|S > x\right]) \geq \frac{\mathbb{E}\left[L\right]}{p_{A_1}}\Bigg\}. \tag{A.6}$$

We also know from Theorem A.1 that the f_1 fraction of nodes that constitute the subnetwork A_1 have their loads and free spaces coming from the updated distributions

$$L^{(1)} \sim L + x_1^\star | S > x_1^\star \tag{A.7}$$

$$S^{(1)} \sim S - x_1^\star | S > x_1^\star. \tag{A.8}$$

We find it useful to denote by Q_i the extra load that each surviving node carries at stage $i = 1, 3, 5, \ldots$, i.e., Q_i denotes the extra load each node in A_i carries. This leads to $Q_1 = x_1^\star$, and we get

$$f_{A_1} = p_{A_1}\mathbb{P}\left[S > Q_1\right] \tag{A.9}$$

where

$$Q_1 = \min\Bigg\{x \in (0,\infty] : \mathbb{P}\left[S > x\right](x + \mathbb{E}\left[L|S > x\right]) \geq \frac{\mathbb{E}\left[L\right]}{p_{A_1}}\Bigg\}. \tag{A.10}$$

Setting $f_{B_0} = p$, $f_{A_{-1}} = 1$, and $Q_{-1} = 0$ for convenience, these establish the desired results (2)–(4) for $i = 0$.

After the intrafailures in network A stabilizes, we check the effect of these on network B, again according to the asynchronous cascading failure model summarized in Fig. 1. Due to the one-to-one interdependence between network A and B, when cascading failures stop at network A, network B reduces to $\bar{B}_2$, which has the same size with A_1; in fact, $\bar{B}_2 = \{b_j : a_j \in A_1\}$. According to our model, the intrafailures in the cyber-network B are governed by the *giant-component* rule, i.e., at each stage a node in B is functional if and only if it belongs to its largest connected component. This will lead to a reduction of $\bar{B}_2$ to its largest connected component, defined as B_2. Due to one-to-one interdependence model, we will next observe $|\bar{B}_2 - B_2|$ nodes failing from network A, more precisely from A_1. It should be clear that the nodes that belong to $|\bar{B}_2 - B_2|$ have failed solely according to the initial intratopology of network B which is constructed independently from network A. Therefore, the removal of $|\bar{B}_2 - B_2|$ nodes from A_1 will be equivalent to a *random* attack launched on A_1 that removes

$$\frac{|\bar{B}_2 - B_2|}{|A_1|} = \frac{|A_1| - |B_2|}{|A_1|} = 1 - \frac{f_{B_2}}{f_{A_1}}$$

fraction of nodes.

As in (2) with $i = 1$, we define $p_{A_3} = \frac{f_{B_2}}{f_{A_1}}$. Now, the impact of intrafailures in network A can be computed once again from Theorem A.1. This time, a random attack of size $1 - p_{A_3}$ will be launched on A_1 whose fractional size is given by f_{A_1}, and the distribution of load and free space of its nodes are as given in (A.7) and (A.8). From Theorem A.1, we get

$$f_{A_3} = f_{A_1}p_{A_3}\mathbb{P}\left[S^{(1)} > x_3^\star\right] \tag{A.11}$$

where $x_3^\star$ is given from

$$x_3^\star = \min\Bigg\{x \in (0,\infty] : \mathbb{P}\left[S^{(1)} > x\right]\left(x + \mathbb{E}\left[L^{(1)}|S^{(1)} > x\right]\right) \geq \frac{\mathbb{E}\left[L^{(1)}\right]}{p_{A_3}}\Bigg\}. \tag{A.12}$$

Also, each surviving node in A_3 will now have an updated load and free-space distribution, given as

$$L^{(3)} \sim L^{(1)} + x_3^\star | S^{(1)} > x_3^\star$$

$$S^{(3)} \sim S^{(1)} - x_3^\star | S^{(1)} > x_3^\star.$$

From (A.7) and (A.8), this is equivalent to

$$L^{(3)} \sim L + Q_3 | S > Q_3 \tag{A.13}$$

$$S^{(3)} \sim S - Q_3 | S > Q_3 \tag{A.14}$$

as we set $Q_3 = x_1^\star + x_3^\star$. As before, Q_3 denotes the extra load that each node in A_3 carries.

We now use (A.7) and (A.8) and definitions of Q_1, Q_3 to simplify (A.11) and (A.12). First, observe that

$$\begin{aligned}\mathbb{P}\left[S^{(1)} > x_3^\star\right] &= \mathbb{P}\left[S - x_1^\star > x_3^\star | S > x_1^\star\right] \\ &= \mathbb{P}\left[S > Q_3 | S > Q_1\right].\end{aligned}$$

Similarly

$$\begin{aligned}&\mathbb{P}\left[S^{(1)}>x\right]\left(x+\mathbb{E}\left[L^{(1)}|S^{(1)}>x\right]\right)\\&=\mathbb{P}\left[S>x_1^\star+x|S>x_1^\star\right]\left(x+\mathbb{E}\left[x_1^\star+L|S>x_1^\star\right]\right)\\&=\frac{\mathbb{P}\left[S>Q_1+x\right]}{\mathbb{P}\left[S>Q_1\right]}\left(x+Q_1+\mathbb{E}\left[L|S>Q_1\right]\right)\end{aligned}$$

since $x>0$. Finally, we have

$$\mathbb{E}\left[L^{(1)}\right]=\mathbb{E}\left[L+x_1^\star|S>x_1^\star\right]=Q_1+\mathbb{E}\left[L|S>Q_1\right].$$

Reporting these into (A.11) and (A.12), we now get

$$f_{A_3}=f_{A_1}p_{A_3}\mathbb{P}\left[S>Q_3|S>Q_1\right] \tag{A.15}$$

where

$$\begin{aligned}Q_3=Q_1+\min\Bigg\{&x\in(0,\infty]:\frac{\mathbb{P}\left[S>Q_1+x\right]}{\mathbb{P}\left[S>Q_1\right]}\\&\times\left(x+Q_1+\mathbb{E}\left[L|S>Q_1\right]\right)\geq\frac{Q_1+\mathbb{E}\left[L|S>Q_1\right]}{p_{A_3}}\Bigg\}.\end{aligned} \tag{A.16}$$

The desired results (2)–(4) of Theorem 3.1 are now established for $i=1$.

The cascade process will continue in the same manner, by considering the failures in network B. Again, the impact of intrafailures in B will be equivalent to a random attack launched at A_3 that fail

$$\frac{|\bar{B}_4-B_4|}{|A_3|}=\frac{|A_3|-|B_4|}{|A_3|}=1-\frac{f_{B_4}}{f_{A_3}}:=1-p_{A_5}$$

fraction of nodes. We can use Theorem A.1 again to compute the fraction of nodes from A_3 that survive this random attack. This time we should note that the fraction of nodes in A_3 equals f_3, while the load and free-space values of nodes in A_3 follow (A.13) and (A.14), respectively. This gives us

$$f_{A_5}=f_{A_3}p_{A_5}\mathbb{P}\left[S^{(3)}>x_5^\star\right] \tag{A.17}$$

where $x_3^\star$ is given from

$$\begin{aligned}x_5^\star=\min\Bigg\{&x\in(0,\infty]:\\&\mathbb{P}\left[S^{(3)}>x\right]\left(x+\mathbb{E}\left[L^{(3)}|S^{(3)}>x\right]\right)\geq\frac{\mathbb{E}\left[L^{(3)}\right]}{p_{A_5}}\Bigg\}.\end{aligned} \tag{A.18}$$

Once again, we can simplify (A.17) and (A.18) using (A.13), (A.13) and setting $Q_5=Q_3+x_5^\star$. We omit the details here in the interest of brevity, but it is straightforward to see that

$$f_{A_5}=f_{A_3}p_{A_5}\mathbb{P}\left[S>Q_5|S>Q_3\right] \tag{A.19}$$

where

$$\begin{aligned}Q_5=Q_3+\min\Bigg\{&x\in(0,\infty]:\frac{\mathbb{P}\left[S>Q_3+x\right]}{\mathbb{P}\left[S>Q_3\right]}\\&\times\left(x+Q_3+\mathbb{E}\left[L|S>Q_3\right]\right)\geq\frac{Q_3+\mathbb{E}\left[L|S>Q_3\right]}{p_{A_5}}\Bigg\}.\end{aligned} \tag{A.20}$$

The results (2)–(4) are now established for $i=2$.

The form of the recursive equations concerning the functional size of network A is now clear: We have (2)–(4) for each $i=0,1,\ldots$ upon setting

$$Q_{2i+1}=\sum_{k=1}^{i}x_{2k+1}^\star=Q_{2i-1}+x_{2i+1}^\star. \tag{A.21}$$

As already mentioned, Q_{2i+1} denotes the extra load that each node in A_{2i+1} carries. Using (2)–(4), we can compute the size, $f_{A_{2i+1}}$ of the functioning nodes in the physical network A at any stage i of the cascading failure process. Next, we will look at how we can compute the size $f_{B_{2i}}$ of functioning component in the cyber-network B.

B. Computing the Giant Component in the Cyber-Network

We now explain how the remaining fraction of functional nodes in the cyber-network B can be computed at each stage of the cascading failures, i.e., we will establish (5)–(7). The main idea we will use in this proof is the fact that the failures that take place in network A at each cascade step due to flow redistribution will be seen as a *random* attack to the remaining portion of network B. This follows from the intratopology of network B being independent from the load and free-space values of the corresponding nodes in A.

With this in mind, the following result established in [21] and [23] will be used repeatedly.

Theorem B.2: Consider a network B generated randomly according to the configuration model with degree distribution $\{d_k\}_{k=0}^{\infty}$, i.e., we have $\mathbb{P}\left[\text{degree of node } b_i=k\right]=d_k$ for each $k=0,1,\ldots$ and $i=1,\ldots,N$. The mean degree is denoted by $\langle d\rangle$, i.e., we have $\langle d\rangle=\sum_{k=0}^{\infty}kd_k$. Let $f_B(p)$ be the *mean* fraction of nodes that are still functioning after a random attack is launched on $(1-p)$-fraction of the nodes in B. In other words, with $\bar{B}$ denoting the network obtained by deleting every node of B independently with probability $(1-p)$, let $f_B(p)$ give the fraction of nodes that are in the giant component of $\bar{B}$. We have

$$f_B(p)=p\left(1-\sum_{k=0}^{\infty}d_k\left(1-u^\star p\right)^k\right) \tag{B.1}$$

where

$$u^\star=\max\left\{u\in[0,1]:u=1-\sum_{k=0}^{\infty}\frac{kd_k}{\langle d\rangle}(1-up)^{k-1}\right\}. \tag{B.2}$$

In (B.1) and (B.2), $u^\star$ gives the probability that a randomly selected edge in $\bar{B}$ leads through one of its end nodes to the giant component of $\bar{B}$.

Theorem B.2 can be used directly to derive (5)–(7) for $i=0$, i.e., to compute the fraction of nodes in B_2. As stated before, the initial attack on $1-p$ fraction of the nodes and subsequent failures in network A due to flow redistribution leads to network A reducing to A_1 whose relative size is given by f_{A_1}. Due to the one-to-one interdependence between networks A and B, this will lead to network B reducing to $\bar{B}_2$, which has the

same size with A_1; in fact, $\bar{B}_2 = \{b_j : a_j \in A_1\}$. In light of the aforementioned independence between the intratopology of network B and the failures that lead A to reduce to A_1, the reduction of B to $\bar{B}_2$ will be equivalent to a random attack launched on B that kills

$$1 - |\bar{B}_2| = 1 - f_{A_1} := p_{B_2}$$

fraction of the nodes. Thus, the size of the giant component of $\bar{B}_2$ (denoted as B_2 with relative size f_{B_2}) can be computed from Theorem B.2 by replacing p with p_{B_2}. This yields

$$f_{B_2} = p_{B_2}\left(1 - \sum_{k=0}^{\infty} d_k \left(1 - u_2 p_{B_2}\right)^k\right)$$

where

$$u_2 = \max\left\{u \in [0,1] : u = 1 - \sum_{k=0}^{\infty} \frac{k d_k}{\langle d \rangle}(1 - u p_{B_2})^{k-1}\right\}.$$

These establish (5)–(7) for $i = 0$.

For the subsequent stages, we use the following result that was introduced in [7]. Let network B be generated as described in Theorem B.2. Assume that, as in the case studied here, B goes through a series of random attacks, where after each attack only the largest connected component of the nonattacked part remains functional. For example, let B go through the following process:

$$B \xrightarrow[(1-p_2)-\text{fraction}]{\text{random attack}} \bar{B}_2 \xrightarrow[\text{comp.}]{\text{giant}} B_2 \xrightarrow[1-p_4]{\text{attack}} \bar{B}_4 \xrightarrow[\text{comp.}]{\text{giant}} B_4$$
$$\rightarrow \cdots \rightarrow B_{2i} \xrightarrow[1-p_{2i+2}]{\text{attack}} \bar{B}_{2i+2} \xrightarrow[\text{comp.}]{\text{giant}} B_{2i+2}. \quad \text{(B.3)}$$

Since all the attacks here are random, this process is equivalent (in terms of the fractional size of B_{2i+2}) to the case where a single random attack (with appropriate size to be discussed next) is applied to B followed by the computation of the giant component of the remaining network. In other words, the process described in (B.3) yields statistically the same fraction of nodes in B_{2i+2} with the process

$$B \xrightarrow[(1-p_2\cdots p_4\cdots p_{2i+2})-\text{fraction}]{\text{random attack}} \bar{B} \xrightarrow[\text{comp.}]{\text{giant}} B_{2i+2}. \quad \text{(B.4)}$$

This result can be understood by considering the point of view of a single fixed node, say v_b in B, and calculating its probability of being in B_{2i+2}. Given that the network is attacked sequentially with probabilities of failing any node being $1 - p_2$, $1 - p_4, \ldots, 1 - p_{2i+2}$, the probability for v_b to *not* fail in any of these stages is given by

$$p_2 \cdots p_4 \cdots p_{2i+2}. \quad \text{(B.5)}$$

This probability is the same with the case if B experiences only one attack that kills $(1 - p_2 \cdot p_4 \cdots p_{2i+2})$-fraction of nodes. Second, v_b will survive this process and will be in B_{2i+2} if it is also in the giant component of the remaining part of B. We know from [21] that B can have at most one component whose fractional size is positive, with all other components having size $o(n)$. This is also true for all the intermediary networks $B_2, B_4, \ldots$. Thus, the process of reducing the network to its giant component can be done only once after all attacks have been applied, without affecting the fractional size of the resulting giant component, i.e., the *small* components (with size $o(n)$) eliminated at each stage in (B.3) will have no affect on the fractional size of B_{2i+2}.

With this result, we can now establish (5)–(7) for all $i = 1, 2, \ldots$. For each i, the fractional size $f_{B_{2i+2}}$ of B_{2i+2} can be computed from Theorem B.2 in view of the equivalence of the processes (B.3) and (B.4). In particular, $f_{B_{2i+2}}$ is calculated from (B.1) and (B.2) as the fractional size of the giant component of $\bar{B}$, obtained by deleting every node of B with probability $1 - p_{B_{2i+2}}$. Here, $p_{B_{2i+2}}$ is the probability for any node in B to not have been attacked in any of the previous stages, and can be computed as in (B.5). In particular, it is given by the multiplication of the probabilities of a node v_b *not* losing its support in network A in consecutive stages. We can compute this probability recursively as

$$p_{B_{2i+2}} = p_{B_{2i}} \mathbb{P}\left[\begin{array}{c} v_b \text{ does not lose its support} \\ \text{in } A \text{ at stage } 2i+1 \end{array}\right]$$
$$= p_{B_{2i}} \frac{|A_{2i+1}|}{|B_{2i}|} \quad \text{(B.6)}$$
$$= p_{B_{2i}} \frac{f_{A_{2i+1}}}{f_{B_{2i}}} \quad \text{(B.7)}$$

where (B.6) follows from the independence of failures in A with the topology of network B. We now established (5) for each $i = 0, 1, \ldots$, and (6) and (7) follow from Theorem B.2 and the discussion that follows.

REFERENCES

[1] R. Albert, H. Jeong, and A.-L. Barabási, "Internet: Diameter of the world-wide web," *Nature*, vol. 401, no. 6749, pp. 130–131, 1999.

[2] J. V. Andersen, D. Sornette, and K.-T. Leung, "Tricritical behavior in rupture induced by disorder," *Phys. Rev. Lett.*, vol. 78, no. 11, pp. 2140–2143, 1997.

[3] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, 1999.

[4] B. Bollobás, "Random graphs," in *Modern Graph Theory*. Berlin, Germany: Springer, 1998, pp. 215–252.

[5] B. Bollobás, *Random Graphs* (Advanced Mathematics). Cambridge, U.K.: Cambridge Univ. Press, 2001.

[6] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[7] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, 2010.

[8] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich, "Interdependent networks with identical degrees of mutually dependent nodes," *Phys. Rev. E*, vol. 83, 2011, Art. no. 016112.

[9] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour, "Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3847–3862, Sep. 2017.

[10] A. Clauset, C. R. Shalizi, and M. E. J. Newman, "Power-law distributions in empirical data," *SIAM Rev.*, vol. 51, no. 4, pp. 661–703, Nov. 2009.

[11] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E*, vol. 69, Apr. 2004, Art. no. 045104.

[12] H. Daniels, "The statistical theory of the strength of bundles of threads. i," *Proc. Roy. Soc. London A, Math., Phys. Eng. Sci.*, vol. 183, pp. 405–435, 1945.

[13] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin, "Robustness of network of networks under targeted attack," *Phys. Rev. E*, vol. 87, May 2013, Art. no. 052804.
[14] R. M. D'souza, "Curtailing cascading failures," *Science*, vol. 358, no. 6365, pp. 860–861, 2017.
[15] P. Erdös and A. Rényi, "On random graphs, i," *Publicationes Mathematicae (Debrecen)*, vol. 6, pp. 290–297, 1959.
[16] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, no. 43, pp. 17–61, 1960.
[17] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Phys.*, vol. 8, no. 1, pp. 40–48, 2012.
[18] T. C. Gulcu, V. Chatziafratis, Y. Zhang, and O. Yağan, "Attack vulnerability of power systems under an equal load redistribution model," *IEEE/ACM Trans. Netw.*, vol. 26, no. 3, pp. 1306–1319, Jun. 2018.
[19] X. Huang, J. Gao, S. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Phys. Rev. E*, vol. 83, 2011, Art. no. 065101.
[20] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari, "Cascaded failures in weighted networks," *Phys. Rev. E*, vol. 84, no. 4, 2011, Art. no. 046114.
[21] M. Molloy and B. Reed, "A critical point for random graphs with a given degree sequence," *Random Struct. Algorithms*, vol. 6, pp. 161–179, 1995.
[22] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, Dec. 2002, Art. no. 065102.
[23] M. E. Newman, "Spread of epidemic disease on networks," *Phys. Rev. E*, vol. 66, no. 1, 2002, Art. no. 016128.
[24] M. E. Newman, "Random graphs with clustering," *Phys. Rev. Lett.*, vol. 103, no. 5, 2009, Art. no. 058701.
[25] M. E. Newman, S. H. Strogatz, and D. J. Watts, "Random graphs with arbitrary degree distributions and their applications," *Phys. Rev. E*, vol. 64, no. 2, 2001, Art. no. 026118.
[26] O. Ozel, B. Sinopoli, and O. Yağan, "Uniform redundancy allocation maximizes the robustness of flow networks against cascading failures," *Phys. Rev. E*, vol. 98, no. 4, 2018, Art. no. 042306.
[27] S. Pahwa, A. Hodges, C. Scoglio, and S. Wood, "Topological analysis of the power grid and mitigation strategies against cascading failures," in *Proc. IEEE Syst. Conf.*, 2010, pp. 272–276.
[28] S. Pahwa, C. Scoglio, and A. Scala, "Abruptness of cascade failures in power grids," *Sci. Rep.*, vol. 4, 2014, Art. no. 3694.
[29] 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, 2010, Art. no. 048701.
[30] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *Int. J. Crit. Infrastructures*, vol. 4, no. 1, pp. 63–79, Jan. 2008.
[31] A. Scala, P. G. D. S. Lucentini, G. Caldarelli, and G. DAgostino, "Cascades in interdependent flow networks," *Physica D, Nonlinear Phenomena*, vol. 323, pp. 35–39, 2016.
[32] E. M. Shahrivar, M. Pirani, and S. Sundaram, "Spectral and structural properties of random interdependent networks," *Automatica*, vol. 83, pp. 234–242, 2017.
[33] E. M. Shahrivar and S. Sundaram, "The game-theoretic formation of interconnections between networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 2, pp. 341–352, Feb. 2017.
[34] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-dependence relations," *Phys. Rev. E*, vol. 83, no. 3, 2011, Art. no. 036116.
[35] A. Vespignani, "Complex networks: The fragility of interdependency," *Nature*, vol. 464, pp. 984–985, 2010.
[36] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the {US} power grid," *Safety Sci.*, vol. 47, no. 10, pp. 1332–1336, 2009.
[37] W.-X. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Phys. Rev. E*, vol. 77, Feb. 2008, Art. no. 026101.
[38] O. Yağan, "Robustness of power systems under a democratic-fiber-bundle-like model," *Phys. Rev. E*, vol. 91, Jun. 2015, Art. no. 062811.
[39] O. Yağan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures and robustness," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1708–1720, Sep. 2012.
[40] Y. Zhang, A. Arenas, and O. Yağan, "Cascading failures in interdependent systems under a flow redistribution model," *Phys. Rev. E*, vol. 97, Feb. 2018, Art. no. 022307.
[41] Y. Zhang and O. Yağan, "Optimizing the robustness of electrical power systems against cascading failures," *Sci. Rep.*, vol. 6, 2016, Art. no. 27625.
[42] Y. Zhang and O. Yağan, "Modeling and Analysis of Cascading Failures in Interdependent Cyber-Physical Systems," in *Proc. 57th IEEE Annu. Conf. Decis. Control*, Dec. 2018, pp. 4731–4738.
[43] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin, "Percolation of partially interdependent scale-free networks," *Phys. Rev. E*, vol. 87, May 2013, Art. no. 052812.

Yingrui Zhang (S'15) received the B.S. degree in electrical engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2011, and the M.S. degree in electrical engineering from Peking University, Beijing, China, in 2014. She is currently working toward the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA.

Her research interests include interdependent systems, robustness and cascading failures in networks, dynamical processes in complex networks, and their applications.

Osman Yağan (S'07–M'12–SM'17) received the B.S. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, in 2007, and the Ph.D. degree in electrical and computer engineering from the University of Maryland, College Park, MD, USA, in 2011.

In August 2013, he joined the faculty of the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, USA, where he is currently an Associate Research Professor. His research interests include modeling, analysis, and performance optimization of computing systems, and uses tools from applied probability, data science, machine learning, and network science. Specific topics include wireless communications, security, random graphs, social and information networks, and cyber-physical systems.

Dr. Yağan is a recipient of the CIT Dean's Early Career Fellowship.