Robustness of Interdependent Cyber-Physical Systems against Cascading Failures

Yingrui Zhang and Osman Yağan

***Abstract*— There is a consensus that integrated cyber-physical systems (CPSs), such as the smart-grid, will emerge as the underpinning technology for major industries. A major concern regarding such systems are the seemingly unexpected large scale failures. Such events 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. This phenomenon, also known as cascade of failures, has the potential of collapsing an entire infrastructure. In this paper, we develop a novel interdependent system model to capture this phenomena. Our framework consists of two networks that have inherently different characteristics governing their *intra*-dependency: i) a *cyber*-network where a node is deemed to be functional as long as it belongs to the largest connected (i.e., giant) component; and ii) a *physical* network where nodes are given an initial *flow* and a *capacity*, and failure of a node results with redistribution of its flow to the remaining nodes, upon which further failures might take place due to *overloading* (i.e., the flow of a node exceeding its capacity). Furthermore, it is assumed that these two networks are *inter-dependent*. For simplicity, we consider a one-to-one interdependency model where every node in the cyber-network is dependent upon and supports a single node in the physical network, and vice versa. We provide a thorough analysis of the dynamics of cascading failures in this interdependent system initiated with a random attack. The system robustness is characterized in terms of all network parameters involved (e.g., degree distribution, load/capacity values, etc.). These analytic results are also supported by a numerical study.**

***Index Terms*— Cascading failures; Robustness; Cyber-physical systems**

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). There is a consensus that integrated cyber-physical systems (CPSs) will emerge as the underpinning technology for major industries in the 21st century. 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 [28] 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 [5]. For example, it was shown [23] that the electrical blackout that affected much of Italy on 28 September 2003 had started with the shutdown of a power station, which led to failures in the Internet communication network, which in turn caused the breakdown of more stations, and so on.

As we embark on a future where interdependent systems are becoming an integral part of our daily lives, a fundamental question arises as to how we can design them in a *robust* and *reliable* manner. Numerous applications of interdependent systems – including those that concern the nation's security, the health care system, monitoring and protecting natural landscapes, the electrical power system, and emergency services – clearly put the successful and efficient operation of them at the core of technologies that are vital to us. To that end, a major focus has to be put on understanding their vulnerabilities, and in particular the root cause of the seemingly unexpected but large scale cascading failures. 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 network science falls short in providing such a characterization since the focus has mainly been on single networks in isolation; i.e., networks that do not interact with, or depend on any other network. Despite some recent research activity aimed at studying interdependent networks [5], [6], [10], [15], [22], [35], very few consider engineering aspects of inter-dependent networks and very little is known as to how such systems can be designed to have maximum robustness under certain design constraints; see [7], [26], [32], [34] for rare exceptions. The current literature is also lacking interdependent system models that capture fundamental differences between *physical* and *cyber* networks, and enable studying robustness of systems that integrate networks with inherently different behavior; e.g., the functionality of the physical subsystem would be primarily governed by the physical flows and capacities associated with its components,

This research was supported by National Science Foundation through grant CCF #1422165.

Y. Zhang and O. Yağan are with the Department of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA, 15213 USA yingruiz@andrew.cmu.edu, oyagan@ece.cmu.edu

while in a cyber-network system-wide connectivity would be the prominent requirement for maintaining functionality. There is thus a need to develop a new approaches for modeling and analyzing cascading failures in interdependent cyber-physical systems.

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 *intra*-dependency models for each constituent network as well as an *inter*-dependency model describing the spread of failures *across* networks; see Section II-A for a detailed discussion on the differences between them. 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 the power grid, *islanding* is a commonly used strategy for preventing cascades [11].

Our interdepedent system model consists of two networks: i) 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 ii) a *physical* network where nodes are given an initial *flow* and a *capacity*, and failure of a node results with redistribution of its flow to the remaining nodes, upon which further failures might take place due to *overloading* (i.e., the flow of a node exceeding its capacity). For simplicity, we consider a one-to-one interdependency model where every node in the cyber-network is dependent upon and supports a single node in the physical network, and vice versa. 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, attack size, etc.). These analytic results are also supported by an extensive numerical study. Interesting findings include the observation that the system tends to go through a complete breakdown through a discontinuous (i.e., first-order) transition with respect to increasing attack size. In other words, the variation of the "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 is reminiscent of large but rare blackouts seen in real world, in a way explaining how small initial shocks can cascade to disrupt large systems that have proven stable with respect to similar disturbances in the past. Finally, we also comment on how system robustness can be improved by properly assigning node capacities in the physical network, when the total capacity of all nodes is fixed.

We believe this work brings a new and fresh perspective to the field of robustness of interdependent networks by steering the literature away from heavily-studied percolation models towards flow-redistribution models, *and* models that combine networks with inherently different cascade characteristics (of which CPS is an arctypal example).

The rest of the paper is organized as follows. In Section II, we present our interdependent system model in details, starting with the distinction between intra-dependency and inter-dependency. In Section III, we present the main result of the 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 Appendix. In Section IV, we present numerical results demonstrating the accuracy of our analysis in the finite node regime. The paper is concluded in Section V with several suggestions for future work.

II. System Model

A. Intra-dependency vs. Inter-dependency

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

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

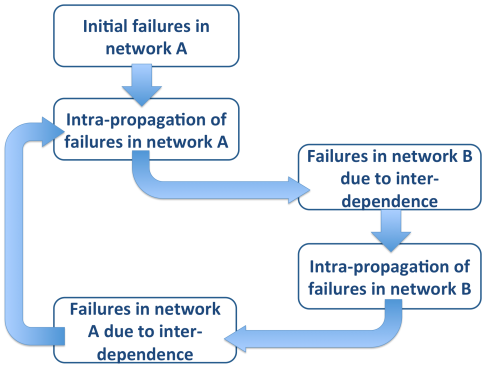

Fig. 1. *An illustration of failure propagation model in an interdependent system.*

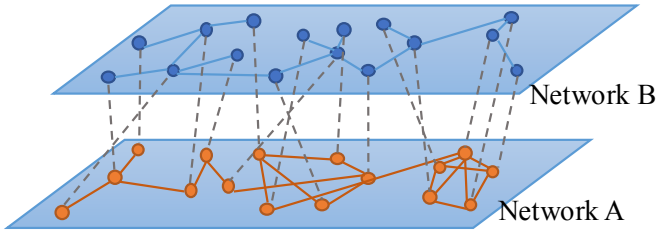

Fig. 2. *System model illustration for the cyber-physical systems, where network A can be the physical grid, and network B can be the communication network that sends control signals. The interdependence across the two networks are realized through random one-to-one support links shown by dashed lines.*

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, either due to random failures, or due to adversarial attacks. To get a better idea about the role of intra- and inter-dependencies in the cascade of failures, consider an *asynchronous* failure update model, where the effect of intra-dependencies and inter-dependencies are considered in two separate batches, following one another. See Figure 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 nodes can not heal once failed.

B. The Model

Despite the vast literature on interdependent networks [5], [25], [32], [33], there has been little (if any) attempt to characterize the robustness of interdependent systems where the constituent networks have different intra-dependency behaviors. In the case of CPS, it would be expected that the cyber and physical counterparts obey inherently different rules governing how failures would propagate internally in each network. To this end, we study in this paper an interdependent system model that consists of two networks with different characteristics governing their *intra*-dependency: i) a *cyber*-network where a node is deemed to be functional as long as it belongs to the largest connected (i.e., giant) component; and ii) a *physical* network where nodes are given an initial *flow* and a *capacity*, and failure of a node results with redistribution of its flow to the remaining nodes, upon which further failures might take place due to *overloading* (i.e., the flow of a node exceeding its capacity). To the best of our knowledge, this is the first work in the literature that studies interdependence between networks with fundamentally different intra-dependency; most existing works are focused on the interdependency between two physical networks (that obey a flow-redistribution-based model) [24], or two cyber-networks (that obey a giant-component-based intra-failure model) [5].

For simplicity, the interdependence across the two networks is assumed to be one-to-one; i.e., every node in the cyber-network is dependent upon and supports a single node in the physical network, and vice versa; see Figure 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; more complicated inter-dependence 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 only function inside each constituent network.

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

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

where S_i denotes the *free-space* (or, redundancy) available to node a_i. It is assumed that a node *fails* (i.e., outages) if its load exceeds its capacity at any given time. The key assumption of our intra-dependency model for network A is that when a node fails, the load it was carrying (right before the failure) is redistributed *equally* among all remaining nodes. This leads to an increase in load carried by all remaining nodes, which in turn may lead to further failures of overloaded nodes, and so on, potentially leading to a cascade of failures.

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.

The equal load redistribution rule takes its roots from the *democratic* fiber bundle model [1], [9], and has been recently used by Pahwa et al. [21] in the context of power systems; see also [31], [34]. The relevance of the equal load-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 the *topological* models where failed load is redistributed only *locally* among neighboring lines [8], [29].

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

Robustness of networks under the giant-component based failure model has been extensively analyzed in the case of *single* networks [2], [19], [20]. The focus has recently been shifted towards *interdependent* networks with the work of Buldyrev et al. [5], where robustness of two interdependent networks, both operating under the giant-component based intra-dependence rule, was studied. Their model, and most works that follow, are unable to capture the true nature of a cyber-physical network, where the cyber-network and the physical-network should obey a different set of rules determining their intra-dependencies.

We define the structure of the network B through its *degree distribution*, namely the probabilities $\{d_k,\ k = 0, 1, \ldots\}$ that an arbitrary node in B has degree k; clearly, we need to have $\sum_{k=0}^{\infty} d_k = 1$. In particular, each node $b_1, \ldots, b_N$ is assigned a degree drawn from the distribution $\{d_k\}_{k=0}^{\infty}$ independently from any other node. Once the degree sequence, $\text{degree}(b_1), \ldots, \text{degree}(b_N)$, of the network is generated, network B is constructed by selecting uniformly at random a graph among all graphs on N nodes with the given degree sequence; see [4], [17], [20] 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 complex networks.

Interdependent System Model. With the intra-dependency models of both networks specified, we adopt a one-to-one inter-dependency model across networks A and B; i.e., nodes a_i and b_i depend on each other for each $i = 1, \ldots, n$. With these in mind, we are interested in understanding the dynamics of cascading failures in this interdependent system, where failures are initiated by attacking a $1 - p$ fraction of nodes from network A. As explained in Figure 1, we assume an asynchronous cascade model, where intra-propagation and inter-propagation of failures are considered in a sequential manner. At any stage $t = 1, \ldots$ of the cascade process, a node a_i in network A will still be functioning if and only if (i) its current flow is less than its capacity; *and* (ii) its counterpart b_i in network B is still functioning (which is equivalent to b_i being contained in the larges connected subgraph of B). Similarly, a node b_j in network B survives cascade step t if and only if i) it belongs to largest connected component of B; and (ii) its counterpart a_j in network A is still functioning (which is equivalent to a_j carrying a flow less than its capacity).

Since the cascade process is monotone, a steady-state will eventually be reached, possibly after all nodes have failed. Let $\mathcal{N}_{\text{surviving}} \subset \{1, \ldots, N\}$ be the set of node id's that are still functioning at the steady state. In other words, the surviving interdependent system will consist of nodes $\{a_i : i \in \mathcal{N}_{\text{surviving}}\}$ where each a_i has more capacity than its flow and $\{b_i : i \in \mathcal{N}_{\text{surviving}}\}$ that constitutes a connected subgraph 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

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

III. Main Result

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

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

We define f_{B_i} similarly as

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

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

Theorem 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 $\mathbb{P}[\text{degree of node } b_i = k] = d_k$ for each $k = 0, 1, \ldots$ and $i = 1, \ldots, N$. Let mean degree be denoted by $\langle d \rangle$, i.e., let $\langle d \rangle = \sum_{k=0}^{\infty} k d_k$. With $f_{B_0} = p_{B_0} = p$, $f_{A_{-1}} = 1$, and $Q_{-1} = 0$, the relative size of the surviving parts of network A and B at each stage of the cascade, initiated by a random attack on $1-p$ fraction of the nodes, can be computed recursively as follows for each $i = 0, 1, \ldots$

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

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

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

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

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

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

The notation used in Theorem 3.1 is summarized in Table III. 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.

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

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

Next, we provide an outline of the proof, while the full details are available in Appendix. In [34], 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 the initial attack size $1-p$, as well as the load and free space distributions $P_{LS}(x, y)$. The results established in [34] 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.

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_i}	fraction $\lvert A_i \rvert / N$ of surviving nodes in A at stage i
f_{B_i}	fraction $\lvert B_i \rvert / N$ of surviving nodes in B at stage i
Q_i	extra load per surviving node in A at stage $i = 1, 3, 5, \ldots$

TABLE I
KEY NOTATION IN THE ANALYSIS OF CASCADING FAILURES

In the failure propagation model described above for interdependent systems, we know that at odd stages, failures from network B can propagate to network A, causing a fraction of nodes to be removed randomly. When new failures take place at the odd stages $t = 2i+1, i = 1, 2, \cdots$, we can treat the nodes left in network A as a new network A_{2i+1}, with the appropriately updated size and load, free-space distributions. The random removal of nodes caused by failures in network B (through the one-to-one interdependency links) from last cascade stage can be viewed as a new random attack that keeps only $p_{A_{2i+1}}$ fraction of nodes alive. Then following the similar approach, we can compute the size of network A, $f_{A_{2i+1}}$, at the end of each time stage when cascading failures stop. One thing to notice is that the load and free-space distributions need to be updated for each new network A_{2i+1}, since the surviving nodes in A_{2i+1} are added with Q_{2i-1} amount of extra load, and at the same time the free-space of each surviving node must be at least Q_{2i-1}. We show in the detailed proof in Appendix that the changes of the distribution can be represented by the initial load and free-space distribution with Q_{2i+1} representing the extra load in each stage. In other words, each time failures propagate

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

Following the same approach, in network B we treat each new failure that comes from network A as a new random attack (or failure) on the existing network B_{2i+2}. For a node in network B to function, it must belong to the largest connected (i.e., giant) component, so actually the functioning network B_{2i+2} at time stage $t = 2i + 2, i = 0, 1, 2, \cdots$ is the giant component after the random attack propagated from network A. A key insight here is that the sequential process of applying a first random attack on the cyber-network, then computing the giant component, and then applying a second random attack and then computing the giant component is *equivalent* to (in terms of the fractional size of the set of nodes that survives) the process where the second random attack is applied directly after the first one without computing the giant component. 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, namely the size of the giant component after randomly removing $1 - p_{B_{2i+2}}$, can be computed using the technique of generating functions [5], [14], [19], [20], [27]. The formula that gives the network size $f_{B_{2i+2}}$ at each time stage $t = 2i + 2$ is given at (6) and (7).

Once we know how to compute final network size $f_{A_{2i+1}}$ and $f_{B_{2i+2}}$, 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 $p_{B_{2i+2}}$ needed in computing $f_{A_{2i+1}}$ and $f_{B_{2i+2}}$, respectively, need to be updated based on the result of the last cascade stage. Collecting, a thorough analysis that reveals a full understanding of the system behavior and robustness during the failure process is presented in equations (2)- (7).

IV. Numerical Results

In this section, we confirm our analytic results through numerical simulations under wide range of parameter choices. For physical networks carrying certain flow such as the power network (network A in our analysis), we consider different combination of commonly known distributions for the load and free-space variables. Throughout, we consider two commonly used families of distributions that are known to occur in various applications: Uniform distribution and

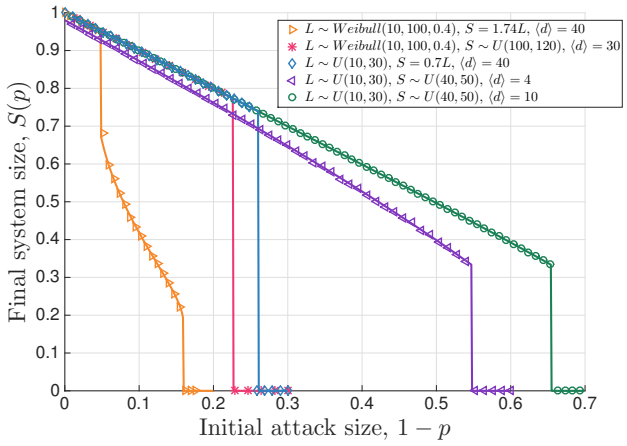

Fig. 3. *Final system size under different network settings, including different load-free space distributions in the physical network and different mean degree in the cyber network. Analytic results are represented by lines, whereas simulation results are represented by symbols (averaged over 20 independent runs). We see that in each case theoretical results match the simulation results very well.*

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

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

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

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

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

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

For the cyber-network where a node is only functional when it belongs to the giant component (network B in the analysis), we model it as an Erdős-Rényi network [3], [12], [13] with average degree $\langle d \rangle$. Erdős-Rényi model is one of the most widely used network models for this type of problem and often serve as the benchmark in various simulations. In our numerical study, we start with N nodes, and with probability $p = \langle d \rangle / N$, we connect each pair of vertices with an edge. When N is large, this is equivalent to generating the network via the configuration model using a *Poisson* degree distribution with mean $\langle d \rangle$. Our analysis is valid under more complicated graphs with arbitrary degree distributions as mentioned in Sec. II. However, for simplicity, we restrict our attention to the ER model in our numerical study.

First, we confirm our numerical results regarding the final system size $S(p)$ presented in Sec. III, i.e. the fraction of

alive nodes when the system is stable after cascading failures caused by an initial 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 20 independent experiments. The results are shown in Figure 3 where symbols represent the *empirical* value of the final system size $S(p)$ (obtained by averaging over 20 independent runs for each data point), and lines represent the analytic results computed from (3) and (6). We see that theoretical results match the simulations very well in all cases. The specific distributions used in Figure 3 are as follows: From left to right, we have i) in network A (the physical network), L is Weibull with $L_{\min} = 10, \lambda = 100, k = 0.4$ and $S = \alpha L$ with $\alpha = 1.74$; in network B (the cyber network) the mean degree $\langle d\rangle = 40$; ii) in network A, L is Weibull with $L_{\min} = 10, \lambda = 100, k = 0.4$ and S is Uniform over $[100, 120]$; in network B $\langle d\rangle = 30$; iii) L is Uniform over $[10, 30]$ and and $S = \alpha L$ with $\alpha = 0.7$; in network B $\langle d\rangle = 40$; iv) L is Uniform over $[10, 30]$ and S is Uniform over $[40, 50]$; $\langle d\rangle = 4$; v)L is Uniform over $[10, 30]$ and S is Uniform over $[40, 50]$; $\langle d\rangle = 10$.

The plots in Figure 3 show how different load-free space distributions in network A as well as the mean degree in network B can affect the system behavior. For example when the mean degree of network B is fixed to $\langle d\rangle = 40$, Weibull distribution (orange triangle) and Uniform distribution (blue diamond) create totally different behavior: Weibull distribution creates a first-then-second order transition before the system size drops to zero through a final first-order transition, while Uniform distribution just gives an abrupt first-order transition at the final breakdown[1]. 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. On the other hand, when we fix the distribution in network A, the change of mean degree from $\langle d\rangle = 4$ (purple triangle) to $\langle d\rangle = 10$ (green circle) brings an increase on the final system size, i.e., the interdependent system becomes more robust. This is quite intuitive since with higher $\langle d\rangle$ value, network B has more connectivity and thus can sustain larger attacks while keeping a relatively large fraction of nodes in the giant component after failures. We can also see that in all cases, the final drop down of the system size is first-order, making it very difficult to predict system behavior (in response to attacks) from previous data. In fact, this is reminiscent of the real-world phenomena of unexpected large-scale system collapses; i.e., cases where seemingly identical attacks/failures leading to entirely different consequences.

From a design perspective, it is desirable to improve or even maximize the robustness of the interdependent systems under certain constrains. Here, we fix the mean degree in network B, and explore the effect of the distribution of node

[1]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.

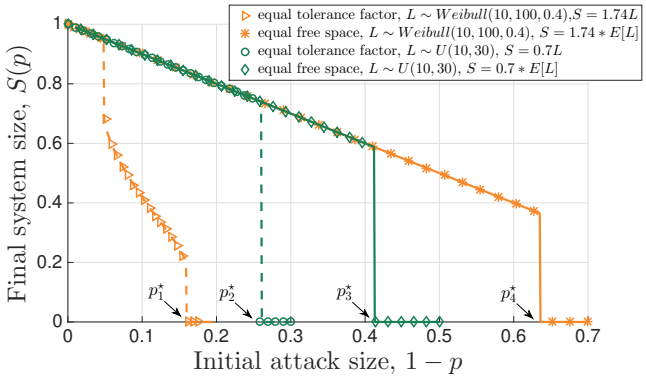

Fig. 4. *Final system size under equal free space or equal tolerance factor when mean degree in network B is fixed. The symbols are empirical results over 20 independent runs on network size $N = 10^5$, and lines (dashed or solid) represent analytical results. $p^\star$ marks the critical attack size above which the system collapse completely. We can see in both cases equal free space greatly improves system robustness by allowing the system to sustain a larger initial attack size, i.e., for Weibull distributed loads, the system can sustain almost four times larger initial attacks (the critical attack size improved from $p_1^\star$ to $p_4^\star$), and when load follows Uniform distribution the robustness is improved for more than 50% (from $p_2^\star$ to $p_3^\star$).*

capacities in the physical network in improving the system robustness. It is evident that the free-space distribution is key to understanding the system robustness as it determines how much extra load a node can take before it fails. In most real world applications, the free space is set to be proportional to the initial load, i.e., $S = \alpha L$, where α is called tolerance factor and is usually a fixed value [8], [16], [18], [30]. We already showed in [34] that in a single flow carrying network, giving every node equal free space will provide a better robustness 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 single flow networks the robustness is shown to be maximized when all nodes are given the same free space.

Our numerical simulations, presented in Figure 4, shows that this 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. To provide an overall evaluation of the system robustness, we define the critical attack size $p^\star$ as the minimum attack size that breaks down the whole system, i.e., it is the initial attack size when system size first drops to zero. So the larger $p^\star$ is, the more robust the system is since it can sustain larger attacks. As shown in Figure 4, when keeping the expected free space $E[S]$ the same (i.e., the total free space in the network is constrained), we see that for Weibull distributions, $p^\star$ increases from $p_1^\star = 0.1616$ to $p_4^\star = 0.636$. This means that compared to the equal tolerance factor scheme, the system can sustain almost four times larger attacks when equal free space strategy is deployed. Similarly, for Uniform distribution, the equal tolerance factors gives $p_2^\star = 0.2586$ whereas equal free space leads to $p_3^\star = 0.4138$, an increase of more than 50%.

V. 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 intra-dependency characteristics. In particular, inspired by many applications of inter-dependent cyber-physical systems (CPSs), our model consists of a flow network where failure of a node leads to flow redistribution and possible further failures due to *overloading* (i.e., the flow on a node exceeding its capacity), and a cyber-network where nodes need to be a part of the largest connected cluster to be functional. We derive relations for the dynamics of cascading failures, characterizing the 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 numerical 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 inter-dependence model used here can be replaced by more sophisticated and realistic dependency model. A good starting point would be to consider the model where every node is assigned k inter-links 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 trade-off between the number of interlinks and the resulting improvements in overall system robustness; one might also consider a heterogeneous allocation of inter-links and study the optimal (in the sense of maximizing robustness) way to assign inter-links subject to certain constraints [32]. It would also be interesting the consider more complicated flow redistribution models based on network topology, rather than the equal redistribution model considered here. Finally, it would be interesting to study the system robustness under targeted attacks (where the set of nodes to be attacked is chosen carefully by an adversary) rather than random attacks.

References

[1] J. V. Andersen, D. Sornette, and K.-t. Leung. Tricritical behavior in rupture induced by disorder. *Physical Review Letters*, 78(11):2140, 1997.

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

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

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

[5] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin. Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291):1025, 2010.

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

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

[8] P. Crucitti, V. Latora, and M. Marchiori. Model for cascading failures in complex networks. *Phys. Rev. E*, 69:045104, Apr 2004.

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

[10] 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*, 87:052804, May 2013.

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

[12] P. Erdös and A. Rényi. On random graphs, i. *Publicationes Mathematicae (Debrecen)*, 6:290–297, 1959.

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

[14] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin. Networks formed from interdependent networks. *Nature physics*, 8(1):40, 2012.

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

[16] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari. Cascaded failures in weighted networks. *Physical Review E*, 84(4):046114, 2011.

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

[18] A. E. Motter and Y.-C. Lai. Cascade-based attacks on complex networks. *Phys. Rev. E*, 66:065102, Dec 2002.

[19] M. E. Newman. Spread of epidemic disease on networks. *Physical review E*, 66(1):016128, 2002.

[20] M. E. Newman, S. H. Strogatz, and D. J. Watts. Random graphs with arbitrary degree distributions and their applications. *Physical review E*, 64(2):026118, 2001.

[21] S. Pahwa, C. Scoglio, and A. Scala. Abruptness of cascade failures in power grids. *Scientific reports*, 4, 2014.

[22] 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.

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

[24] A. Scala, P. G. D. S. Lucentini, G. Caldarelli, and G. DAgostino. Cascades in interdependent flow networks. *Physica D: Nonlinear Phenomena*, 323:35–39, 2016.

[25] E. M. Shahrivar, M. Pirani, and S. Sundaram. Spectral and structural properties of random interdependent networks. *Automatica*, 83:234–242, 2017.

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

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

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

[29] J.-W. Wang and L.-L. Rong. Cascade-based attack vulnerability on the {US} power grid. *Safety Science*, 47(10):1332 – 1336, 2009.

[30] W.-X. Wang and G. Chen. Universal robustness characteristic of weighted networks against cascading failure. *Phys. Rev. E*, 77:026101, Feb 2008.

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

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

[33] Y. Zhang, A. Arenas, and O. Yağan. Cascading failures in interdependent systems under a flow redistribution model. *Phys. Rev. E*, 97:022307, Feb 2018.

[34] Y. Zhang and O. Yağan. Optimizing the robustness of electrical power systems against cascading failures. *Scientific reports*, 6, 2016.

[35] D. Zhou, J. Gao, H. E. Stanley, and S. Havlin. Percolation of partially interdependent scale-free networks. *Phys. Rev. E*, 87:052812, May 2013.

APPENDIX
PROOF OF THE MAIN RESULT

A. Computing the Functional Component in Physical Network

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. The authors' previous work [34] analyzed the cascading failures in a single flow network, and can be used there to compute i) the fraction of additional nodes that will fail as a result of load redistribution cascades; and ii) the extra load that each surviving line will be carrying, once the *steady-state* is reached for the purposes of intra-failures in network A. Of course, for the model under consideration, further failures might take place due to interdependence with network B, which we will discuss later. Let $L^{(1)}$ and $S^{(1)}$ denote random variables following the original load and free space distributions, i.e., $L^{(1)}, S^{(1)} \sim p_{LS}(x,y)$. Then, we know from [34] that the fraction of nodes that are still functioning when the intra-failures in network A stops is given by

$$n_{A_1} = p_{A_1}\mathbb{P}\left[S^{(1)} > x_1^\star\right] \tag{A.1}$$

where $x_1^\star$ denotes the smallest x in $(0,\infty)$ that satisfies the inequality

$$\mathbb{P}\left[S^{(1)} > x\right]\left(x + \mathbb{E}\left[L^{(1)} \mid S^{(1)} > x\right]\right) \geq \frac{\mathbb{E}\left[L^{(1)}\right]}{p_{A_1}} \tag{A.2}$$

If (A.2) does not hold for any x in $(0,\infty)$, we set $x_1^\star = \infty$.

In words, x represent the possible extra load per alive node at each step during the cascading failure process, by finding the smallest solution, i.e. $x_1^\star$, we find the minimum extra load per alive node at which no further failure will happen. In other words, the extra load per alive node will remain $x_1^\star$ since the network is stable and no further failure will happen. Detailed explanation and derivation can be found in [34]. The current network size in network A is

$$N_{A_1} = n_{A_1} * N \tag{A.3}$$

Notice that $x_1^\star$ is also the extra load per node when cascading failure stops after randomly attacking $1-p_{A_1}$ fraction of nodes initially. In other words, the nodes that survive the cascading failure caused by random attack of size $1-p_{A_1}$ must be unattacked from the beginning *and* have at least $x_1^\star$ amount of free space.

Let A_1 be the set of alive nodes when network A is stable after random attack of size $1-p_{A_1}$. As we mentioned before, due to the interdependent relationships between network A and B, when cascading failures stop at network A, not only all the failed nodes are removed from network A (including the initial failed ones and the ones that fail subsequently due to excess load), all their dependent nodes in network B will also be removed due to the one-to-one coupling links between the two networks. So at time stage $t=2$, network B fragments into network $\bar{B}_2$ which is the same size as A_1. Remember that not all nodes left are functional, only the ones that belong to the giant component B_2 can function normally. The functioning nodes in B_2 is a subset of $\bar{B}_2$, i.e., $B_2 \subseteq \bar{B}_2$, then due to the interdependent relations, all nodes that don't belong to the giant component B_2 will be removed (see Fig.xx for illustration).

At time stage $t=3$, the dependent nodes of the $|\bar{B}_2| - |B_2|$ nodes removed in last time stage will be removed in network A. Because the one-to-one support links between two networks are random, the removal of the dependent links can be seen as another random attack in the remainings A_1 that survived the initial attack $1-p_{A_1}$. Suppose this random attack kills $1-p_{A_3}$ fraction of nodes in A_1 (we will compute p_{A_3} in Sec. C when computing giant component size in cyber networks). Namely, after network A is stable from the initial attack (or first attack) of size $1-p_{A_1}$, another random attack is deployed in the remaining nodes that survived the first attack.

Before the random attack that removes $1-p_{A_3}$ fraction of nodes, we can see that the remaining network A_1 is a network of size N_1 given by equation (A.3), and the load on each surviving node follows distribution $L^{(3)} \sim L^{(1)} + x_1^\star$, and free space follows distribution $S^{(3)} \sim S^{(1)} - x_1^\star \mid S^{(1)} > x_1^\star$. Using again the results in [34] and treat the remaining network A_1 as a new network, we know that at the stable network size n_3 after the random attack that keeps only p_{A_3} fraction of nodes in A_1 is:

$$n_{A_3} = p_{A_3}\mathbb{P}\left[S^{(3)} > x_3^\star\right] \tag{A.4}$$

where $x_3^\star$ is the smallest solution of the inequality

$$\mathbb{P}\left[S^{(3)} > x\right]\left(x + \mathbb{E}\left[L^{(3)} \mid S^{(3)} > x\right]\right) \geq \frac{\mathbb{E}\left[L^{(3)}\right]}{p_{A_3}}, \tag{A.5}$$

over x in $(0,\infty)$.

Since $L^{(3)}$ is a new random variable that is a constant increment of the original load distribution $L^{(1)}$ (or L), i.e. $L^{(3)} \sim L^{(1)} + x_1^\star$, we know that

$$\mathbb{E}\left[L^{(3)}\right] = \mathbb{E}\left[L^{(1)} + x_1^\star\right] = \mathbb{E}\left[L\right] + x_1^\star \tag{A.6}$$

Similarly, $S^{(3)}$ is a new random variable that is the original random variable for free space $S^{(1)}$ minus a fixed amount, i.e. $S^{(3)} \sim S^{(1)} - x_1^\star \mid S^{(1)} > x_1^\star$, so we have

$$\begin{aligned}\mathbb{P}\left[S^{(3)} > x\right] &= \mathbb{P}\left[S^{(1)} - x_1^\star > x \mid S^{(1)} > x_1^\star\right] \\ &= \frac{\mathbb{P}\left[S - x_1^\star > x, S > x_1^\star\right]}{\mathbb{P}\left[S > x_1^\star\right]} \\ &= \frac{\mathbb{P}\left[S > x_1^\star + x\right]}{\mathbb{P}\left[S > x_1^\star\right]}\end{aligned} \tag{A.7}$$

since $x > 0$.

We know that $L^{(3)}$ and $S^{(3)}$ are related to the initial load $L^{(1)}$ and free space $S^{(1)}$, so the conditional expectation in (A.2) can be simplified as:

$$\begin{aligned}\mathbb{E}\left[L^{(3)} \mid S^{(3)} > x\right] &= \mathbb{E}\left[L^{(1)} + x_1^\star \mid S^{(1)} > x + x_1^\star\right] \\ &= x_1^\star + \mathbb{E}\left[L \mid S > x + x_1^\star\right] \end{aligned} \tag{A.8}$$

Since the possible extra load per alive node x is always greater than zero, the condition $S^{(1)} > x + x_1^\star$ in the above expectation implies that $S^{(1)} > x_1^\star$. $x_1^\star$ is a constant representing the extra load per alive node when cascading failure at initial attack p_1 stops, so we can easily move it out from the expectation.

Bring equations (A.6-A.8) back to (A.2), we have

$$\frac{\mathbb{P}\left[S > x_1^\star + x\right]}{\mathbb{P}\left[S > x_1^\star\right]}(x + x_1^\star + \mathbb{E}\left[L \mid S > x + x_1^\star\right] \geq \frac{\mathbb{E}\left[L\right] + x_1^\star}{p_{A_3}} \tag{A.9}$$

The stable network size n_{A_3} at stage 3, p_{A_3} in (A.1) can also be simplified using (A.7):

$$n_{A_3} = p_{A_3} * \frac{\mathbb{P}\left[S > x_3^\star + x_1^\star\right]}{\mathbb{P}\left[S > x_1^\star\right]} \tag{A.10}$$

where $x_3^\star$ is the smallest solution of (A.9). And the number of alive nodes at this time is

$$N_{A_3} = n_{A_3} * N_{A_1} \tag{A.11}$$

Let A_3 denote the set of alive nodes that survived the cascading failure caused by the random attack at $t = 3$ of size p_{A_3}. At $t = 4$, further nodes failures will happen in network B due to the interdependent links, and this in return results another fraction of nodes being removed in network A at $t = 5$. Notice that the updates and removal of nodes in network A always happen in even time stage, so the subscript of notations in network A are all even numbers. As before, we can regard the removal at $t = 5$ as a random attack that removes $1 - p_{A_5}$ fraction of nodes in the remaining network A_3 from the last random attack, then following the same strategy, we can treat A_3 as a new network with size N_3, and load follows distribution $L^{(5)} \sim L^{(3)} + x_3^\star$, free space follows distribution $S^{(5)} \sim S^{(3)} - x_3^\star \mid S^{(3)} > x_3^\star$. Then the network size after randomly attacking $1 - p_{A_1}$, then $1 - p_{A_3}$ among the alive ones, then $1 - p_{A_5}$ among the further alive ones, is given by

$$n_{A_5} = p_{A_5}\mathbb{P}\left[S^{(5)} > x_5^\star\right] \tag{A.12}$$

where $x_5^\star$ denotes the smallest x in $(0, \infty)$ that satisfies the inequality

$$\mathbb{P}\left[S^{(5)} > x\right]\left(x + \mathbb{E}\left[L^{(5)} \mid S^{(5)} > x\right]\right) \geq \frac{\mathbb{E}\left[L^{(5)}\right]}{p_{A_5}} \tag{A.13}$$

Breaking each item in (A.13), we see that

$$\begin{aligned}\mathbb{P}\left[S^{(5)} > x\right] &= \mathbb{P}\left[S^{(3)} - x_3^\star > x \mid S^{(3)} > x_3^\star\right] \\ &= \frac{\mathbb{P}\left[S^{(3)} - x_3^\star > x, S^{(3)} > x_3^\star\right]}{\mathbb{P}\left[S^{(3)} > x_3^\star\right]} \\ &= \frac{\mathbb{P}\left[S^{(3)} - x_3^\star > x\right]}{\mathbb{P}\left[S^{(3)} > x_3^\star\right]} \\ &= \frac{\mathbb{P}\left[S^{(3)} > x_3^\star + x\right]}{\mathbb{P}\left[S^{(3)} > x_3^\star\right]} \\ &= \frac{\frac{\mathbb{P}[S > x_3^\star + x_1^\star + x]}{\mathbb{P}\left[S > x_1^\star\right]}}{\frac{\mathbb{P}\left[S > x_3^\star + x_1^\star\right]}{\mathbb{P}\left[S > x_1^\star\right]}} \\ &= \frac{\mathbb{P}\left[S > x_1^\star + x_3^\star + x\right]}{\mathbb{P}\left[S > x_1^\star + x_3^\star\right]} \end{aligned} \tag{A.14}$$

using (A.7). And the conditional expectation becomes

$$\begin{aligned}&\mathbb{E}\left[L^{(5)} \mid S^{(5)} > x\right] \qquad (A.15)\\ &= \mathbb{E}\left[L^{(3)} + x_3^\star \mid S^{(3)} > x + x_3^\star\right] \\ &= \mathbb{E}\left[L^{(1)} + x_3^\star + x_1^\star \mid S^{(1)} > x + x_3^\star + x_1^\star\right] \\ &= x_3^\star + x_1^\star + \mathbb{E}\left[L \mid S > x + x_3^\star + x_1^\star\right] \qquad (A.16)\end{aligned}$$

Using (A.14) and (A.15) in (A.13), we have

$$\begin{aligned}&\frac{\mathbb{P}\left[S > x_1^\star + x_3^\star + x\right]}{\mathbb{P}\left[S > x_1^\star + x_3^\star\right]}(x + x_3^\star + x_1^\star + \mathbb{E}\left[L \mid S > x + x_3^\star + x_1^\star\right]) \\ &\geq \frac{x_1^\star + x_3^\star + \mathbb{E}\left[L\right]}{p_{A_5}}\end{aligned} \tag{A.17}$$

The stable network size n_{A_5} after the randomly attack p_{A_5} in (A.12) can also be simplified using equation (A.14):

$$\begin{aligned}n_{A_5} &= p_{A_5} * \mathbb{P}\left[S^{(5)} > x_5^\star\right] \\ &= p_{A_5} * \frac{\mathbb{P}\left[S > x_1^\star + x_3^\star + x_5^\star\right]}{\mathbb{P}\left[S > x_1^\star + x_3^\star\right]}\end{aligned} \tag{A.18}$$

where $x_1^\star$ and $x_3^\star$ are constant acquired from the first two attacks, and $x_5^\star$ is the smallest solution of (A.17). And the number of alive nodes at this time is

$$N_{A_5} = n_{A_5} * N_{A_3} \tag{A.19}$$

Define Q_{2i-1} as the cumulative extra load on the alive nodes after the i^{th} attack that removes $1 - p_{A_{2i-1}}$ fraction of nodes on the remaining network:

$$Q_{2i-1} = \sum_{k=1}^{i} x_{2k-1}^\star, \qquad i = 1, 2, 3, ... \tag{A.20}$$

Q_{2i-1} is just the summation of a sequence of constants that represent the extra load per alive line when the steady state is reached after each random attack. And $Q_{2i+1} = Q_{2i-1} + x_{2i+1}^\star$, where $x_{2i+1}^\star$ needs to be solved from the equations in the current equivalent random attack that removes $1 - p_{A_{2i+1}}$ fraction of nodes.

Then the recursive relations are clear: the final network size after applying $i+1$ random attacks of size $1-p_{A_1}$, $1-p_{A_3}$, $\cdots$, $1-p_{A_{2i+1}}$ on the remaining network is given by

$$\begin{aligned} n_{A_{2i+1}} &= p_{A_{2i+1}} * \mathbb{P}\left[S^{(2i+1)} > x^{\star}_{2i+1}\right] \\ &= p_{A_{2i+1}} * \frac{\mathbb{P}\left[S > Q_{2i+1}\right]}{\mathbb{P}\left[S > Q_{2i-1}\right]} \end{aligned} \tag{A.21}$$

where Q_{2i-1} is constant acquired from previous steps, and $Q_{2i+1} = Q_{2i-1} + x^{\star}_{2i+1}$, where $x^{\star}_{2i+1}$ is the smallest solution of

$$\begin{aligned} &\frac{\mathbb{P}\left[S > Q_{2i-1} + x\right]}{\mathbb{P}\left[S > Q_{2i-1}\right]}(x + Q_{2i-1} + \mathbb{E}\left[L \mid S > x + Q_{2i-1}\right]) \\ &\geq \frac{Q_{2i-1} + \mathbb{E}\left[L\right]}{p_{A_{2i+1}}} \end{aligned} \tag{A.22}$$

The number of alive nodes $N_{A_{2i+1}}$ after the $(i+1)^{th}$ randomly attack that removes $1-p_{A_{2i+1}}$ fraction of nodes in the remaining network is:

$$N_{A_{2i+1}} = n_{A_{2i+1}} * N_{A_{2i-1}} \tag{A.23}$$

Now $N_{A_{2i+1}}$ gives us the size of the functioning nodes in physical network A at any stage during the interdependent cascading failure process, we will next look at how to compute the size of functioning component in the cyber network.

B. Computing Giant Component in Cyber Network

Since the one-to-one coupling links between two networks are completely random, each time the removal of nodes (in network A or B) brought by the failures of the other network (network B or A) through these support links can be seen as random attacks inside the sub-network. So as before, we will compute the functioning giant component in the cyber network, then introduce the iterative relations in the interdependent system.

Suppose network B is a cyber network with degree distribution p_k and size N, the same size as network A. As stated before, the first removal and updates in network B occurs at time $t=2$, where the effect of removal can be seen as a random attack that removes $1-p_{B_2}$ fraction of nodes (the subscript in p_{B_2} is consistent with the time stage number $t=2$, same as in network A, so in network B all the subscripts are odd number). For the convenience of notation, let $p = p_{B_2}$ be the probability that a node remains in the equivalent random attack at $t=2$ (which is also the initial random attack in network B). After this initial attack in network B, the remaining network $\bar{B}_2$ has size pN. As in [5], [14], [19], [20], [27], we use the techniques of generating functions to compute the giant component $B_2 \subseteq \bar{B}_2$. Define the generating function of the degree distribution in network B as

$$G_0(z) = \sum_{k=0}^{\infty} p_k z^k \tag{B.24}$$

Analogously, we introduce the generating function of the underlying branching processes as

$$G_1(z) = \frac{G_0'(z)}{G_0'(1)} \tag{B.25}$$

where $G_0'(1)$ is the mean degree calculated by $G_0'(1) = \sum_k k p_k = \langle k \rangle$.

Random removal of $1-p$ nodes will change the distribution of the remaining nodes, as a result, the generating function of the new distribution is equal to the generating function of the original distribution with argument $1-p(1-z)$ [19]. Then the fraction of nodes that belong to the giant component B_2 of network $\bar{B}_2$ is given by

$$g_B(p) = 1 - G_0[1 - p(1-u)] \tag{B.26}$$

where u is a function of p satisfying

$$u = G_1[1 - p(1-u)] \tag{B.27}$$

So the functioning giant component has size

$$|B_2| = g_B(p) * p * N \tag{B.28}$$

Now suppose at $t=4$, another equivalent random attack happens in the giant component B_2 as a result of failure happened in network A at $t=3$, which removes $1-p_{B_4}$ fraction of nodes. The remaining network $\bar{B}_4$ is of size $p_{B_4} * |B_2|$, and we want to find the size of the functioning giant component $B_4 \subseteq \bar{B}_4$. The effect of randomly remove $1-p_{B_4}$ fraction of nodes in B_2 have the same effect as taking out the same portion from $\bar{B}_2$, i.e. the remaining network after initial attack of size p [5]. In other words, this second removal is equivalent to the removal of $(1-p_{B_4})$ fraction of nodes from $\bar{B}_2$, which is $p*(1-p_{B_4})$ fraction from the original network B. As $1-p$ fraction of nodes are already removed in the initial attack, the effect of the random attack at $t=2$ and $t=4$ can be seen as an initial attack of size $(1-p)+p*(1-p_{B_4}) = 1-p*p_{B_4}$. Or, the effect of the random attack at $t=4$ is equivalent to a random attack in which p is replaced by $p'_{B_4} = p * p_{B_4}$. So the giant component B_4 after the second attack is

$$|B_4| = g_B(p'_{B_4}) * p'_{B_4} N \tag{B.29}$$

When another equivalent random attack happens in network B at $t=6$ due to failures of network A from last time stage $t=5$, $1-p_{B_6}$ fraction of nodes are removed from network B_4. The remaining network $\bar{B}_6$ is of size $p_{B_6} * |B_4|$. Using a similar approach, we can equivalent this attack on network B_4 as one on the network that removes $1-p'_{B_4}$ fraction of nodes from the original network. As a result, effect of the random attack at $t=6$ is equivalent to an initial removal of size $(1-p'_{B_4}) + p'_{B_4} * (1-p_{B_6}) = 1 - p'_{B_4} * p_{B_6}$, i.e. this is equivalent to an initial random attack in which p is replace by $p'_{B_6} = p'_{B_4} * p_{B_6}$. And the size of the functioning giant component $B_6 \subseteq \bar{B}_6$ is given by

$$|B_6| = g_B(p'_{B_6}) * p'_{B_6} N \tag{B.30}$$

Follow this pattern, we can see that the effect of the i^{th} random attack that removes $1-p_{B_{2i}}$ fraction of nodes on the functioning giant component of network B can be seen as an initial attack where p is replaced by

$$p'_{B_{2i}} = p'_{B_{2i-2}} * p_{B_{2i}}, \qquad i = 1, 2, 3, ... \tag{B.31}$$

and the size of the functioning giant component at this stage is

$$|B_{2i}| = g_B(p'_{B_{2i}}) * p'_{B_{2i}} N \tag{B.32}$$

Now we know what happens when consecutive random failures (or attacks) happen in network B, we can bring two networks together and analyse the iteration relations in the interdependent system.

C. Iteration Relations in the System

When the cyber network is coupled with the physical network, at each stage, failures in the physical network (network A) will result the same fraction of nodes being removed in the cyber network (network B), due to the one-to-one dependent links. Similarly, each time failure happens in the cyber network, the same fraction of nodes will be removed in the physical network. Let p_{A_t} and p_{B_t} denote the fraction of nodes that *stays* in the network when random attack (or failure) happens, i.e., $1-p_{A_t}$ or $1-p_{B_t}$ fraction of nodes are removed in every random attack at stage t. Also define f_{A_t} and f_{B_t} as the size of the functioning component in each network at stage t, or the fraction of nodes that remains functioning.

Initially at $t=1$, random attacks happen in a network. Without loss of generality, we assume that the attacks starts in network A (we can follow the same analysis if random attacks start in network B). So at the beginning, network A experiences a random attack that removes $1-p_{A_1}$ fraction of nodes. The failure of these nodes will cause load redistribution, and further failure may occur as a result, leading to a cascade of failures. When cascading failures stop, the remaining network A_1 is the functioning component of size f_{A_1} which can be solved from equations (A.1) and (A.2):

$$f_{A_1} = n_{A_1} = p_{A_1}\mathbb{P}\left[S^{(1)} > x_1^\star\right] \tag{C.33}$$

and the number of nodes in the functioning component is $|A_1| = f_{A_1} * N$.

At $t=2$, failures happen in network A will affect network B through the one-to-one interdependent links. That is to say, now network A lost $1-f_{A_1}$ fraction of nodes, the nodes in network B that depend on these failed nodes will also be removed. Since nodes in network A and B are inter-linked randomly, we can equivalent this effect of failures in network B as a random attack that keeps only $p_{B_2} = f_{A_1}$ fraction of nodes alive. After this random attack, the remaining network $\bar{B}_2$ has size $p_{B_2}N$. The size of the functioning giant component $B_2 \subseteq \bar{B}_2$ can be computed from equations (B.26) - (B.28):

$$f_{B_2} = g_B(p_{B_2}) * p_{B_2} \tag{C.34}$$

and the number of nodes in B_2 is $|B_2| = f_{B_2} * N$.

For network B, besides the initial attack that removes $1-p_{B_2}$ fraction of nodes, another $|\bar{B}_2| - |B_2| = (f_{A_1} - f_{B_2}) * N$ nodes are removed. So at $t=3$, this additional amount of nodes will be removed in the remaining network A_1. The removal is equivalent to a random attack on A_1 that keeps only p_{A_3} fraction of nodes alive, where

$$p_{A_3} = 1 - \frac{|\bar{B}_2| - |B_2|}{|A_1|} = 1 - \frac{f_{A_1} - f_{B_2}}{f_{A_1}} = \frac{f_{B_2}}{f_{A_1}} \tag{C.35}$$

After randomly remove $1-p_{A_3}$ fraction of nodes in A_1, network A is left with $\bar{A}_3 = p_{A_3} * |A_1|$ nodes. Note that $\bar{A}_3$ is the same size as B_2 from the last time stage, i.e., $|B_2| = |\bar{A}_3|$, because the two networks are kept with the same size at the beginning of each time stage due to the one-to-one interdependent links. Further failure will happen in $\bar{A}_3$ due to load redistribution, and when failures stop, network A is left with a functioning component $A_3 \subseteq \bar{A}_3$ of size n_{A_3}:

$$n_{A_3} = p_{A_3}\mathbb{P}\left[S^{(3)} > x_3^\star\right] \tag{C.36}$$

and the number of nodes in the current functioning component of network A is $|A_3| = n_{A_3} * |A_1| = f_{A_3} * N$, where $f_{A_3} = n_{A_3} * n_{A_1}$.

At $t=4$, all the dependent nodes in network B of the nodes failed from last stage in network A will be removed, which is $(|\bar{A}_3| - |A_3|)/|\bar{A}_3|$ fraction on network B_2 (recall that $|B_2| = |\bar{A}_3|$). This is equivalent to a random attack that keeps only p_{B_4} fraction of nodes in network B_2:

$$p_{B_4} = 1 - \frac{|\bar{A}_3| - |A_3|}{|\bar{A}_3|} = 1 - \frac{p_{A_3} - n_{A_3}}{p_{A_3}} = \frac{n_{A_3}}{p_{A_3}} \tag{C.37}$$

After the random attack at $t=4$, the remaining network $\bar{B}_4$ is of size $p_{B_4} * |B_2|$, which is the same size as A_3 from last time stage.

As we show in Sec.B, the effect of attacking $1-p_{B_4}$ randomly in B_2 is equivalent to remove the same fraction from $\bar{B}_2$, hence the effect of the 4^{th} stage failure in network B is equivalent to a random attack in which p is replaced by $p'_{B_4} = p_{B_2} * p_{B_4}$. Following the same analysis, we can get the size of the functioning giant component $B_4 \subseteq \bar{B}_4$:

$$f_{B_4} = g_B(p'_{B_4}) * p'_{B_4} \tag{C.38}$$

and the number of nodes in the functioning giant component B_4 is $|B_4| = f_{B_4} * N$.

At $t=5$, the additional amount of nodes to be removed in network A is $(|\bar{B}_4| - |B_4|)/|\bar{B}_4| = (|A_3| - |B_4|)/|A_3|$ (recall that $|\bar{B}_4| = |A_3|$), which is equivalent to a random attack that keeps only p_{A_5} fraction of nodes in network A_3:

$$p_{A_5} = 1 - \frac{|A_3| - |B_4|}{|A_3|} = 1 - \frac{f_{A_3} - f_{B_4}}{f_{A_3}} = \frac{f_{B_4}}{f_{A_3}} \tag{C.39}$$

After randomly removing $1-p_{A_5}$ fraction of nodes in A_3, the remaining network $\bar{A}_5$ is of size $p_{A_5} * |A_3|$. After the redistribution followed by the failure, more nodes may fail, and when failure stops, network A is left with the functioning component $A_5 \subseteq \bar{A}_5$ of size n_{A_5}:

$$n_{A_5} = p_{A_5}\mathbb{P}\left[S^{(5)} > x_5^\star\right] \tag{C.40}$$

and the number of nodes in the current functioning component of network A is $|A_5| = n_{A_5} * |A_3| = f_{A_5} * N$, where $f_{A_5} = n_{A_5} * n_{A_3} * n_{A_1}$.

At $t = 6$, $(|\bar{A}_5| - |A_5|)/|\bar{A}_5|$ fraction of nodes will be removed from the functioning giant component B_4 in network B, due to the failures happened in network A from last time stage. This is equivalent to a random attack on B_4 that keeps only p_{B_6} fraction of nodes in the functioning giant component:

$$p_{B_6} = 1 - \frac{|\bar{A}_5| - |A_5|}{|\bar{A}_5|} = 1 - \frac{p_{A_5} - n_{A_5}}{p_{A_5}} = \frac{n_{A_5}}{p_{A_5}} \quad \text{(C.41)}$$

After removing $1 - p_{B_6}$ fraction of nodes from B_4, the remaining network $\bar{B}_6$ is of size $p_{B_6} * |B_4|$ (note that $|\bar{B}_6| = |A_5|$). Combining the removal of $1 - p_{B_6}$ fraction and the $1 - p'_{B_4}$ fraction from the previous failure in network B, the effect is equivalent to a initial random attack that only keeps $p'_{B_6} = p'_{B_4} * p_{B_6}$ fraction of nodes from the original network. So the size of the functioning giant component at this stage $B_6 \subseteq \bar{B}_6$ is given by

$$f_{B_6} = g_B(p'_{B_6}) * p'_{B_6} \quad \text{(C.42)}$$

and the number of nodes in the functioning giant component B_6 is $|B_6| = f_{B_6} * N$.

Now the iterative relations in the system is clear: initially at $t = 1$, $1 - p_{A_1}$ fraction of nodes are attacked randomly in network A; at $t = 2$, only $p_{B_2} = f_{A_1}$ fraction nodes are left in network B, then at odd time stage we update network A: For each $i = 0, 1, \ldots,$

$$p_{A_{2i+1}} = \frac{f_{B_{2i}}}{f_{A_{2i-1}}} \quad \text{(C.43)}$$

$$n_{A_{2i+1}} = p_{A_{2i+1}} \mathbb{P}\left[S^{(2i+1)} > x^{\star}_{2i+1}\right] \quad \text{(C.44)}$$

$$f_{A_{2i+1}} = f_{A_{2i-1}} n_{A_{2i+1}} = n_{A_1} \cdot n_{A_3} \cdots n_{A_{2i+1}} \quad \text{(C.45)}$$

and at even time stage we update network B:

$$p_{B_{2i+2}} = \frac{n_{A_{2i+1}}}{p_{A_{2i+1}}} = \frac{n_{A_{2i+1}} f_{A_{2i-1}}}{f_{B_{2i}}} = \frac{f_{A_{2i+1}}}{f_{B_{2i}}} \quad \text{(C.46)}$$

$$p'_{B_{2i+2}} = p'_{B_{2i}} * p_{B_{2i+2}} \quad \text{(C.47)}$$

$$f_{B_{2i+2}} = g_B(p'_{B_{2i+2}}) * p'_{B_{2i+2}} \qquad i = 1, 2, .. \quad \text{(C.48)}$$

This iterative relation stops when neither network A nor network B fragment further, i.e., when $f_{A_{2i-1}} = f_{A_{2i+1}}$ and $f_{B_{2i}} = f_{B_{2i+2}}$.