The Aftermath of Broken Links: Resilience of IoT Systems from A Networking Perspective

Sigit Pambudi*, Jie Wang*, Wenye Wang*, Min Song†, Xiaoyan Zhu‡
*Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606
†Department of Computer Science, Michigan Technological University, MI 49931
‡National Key Laboratory of Integrated Networks Services, Xidian University, Xi'an, 710071, China
{spambudi, jwang50, wwang}@ncsu.edu, mins@mtu.edu, xyzhu@mail.xidian.edu.cn

Abstract—**Internet of things (IoT) is expected to provide a fully informative and controllable environment that features networking, automation, and intelligence by interconnecting physical systems to cyber world. Such a correlation opens the interdependence between the two, so that a single incident in one domain, *e.g.*, a broken communication link, or an out-of-battery device, can cause a cascade-of-failures across physical and cyber domains. To understand the *resilience* of IoT systems against such detrimental cascades, this paper studies the aftermath of edge and jointly-induced cascades, that is, a sequence of failures induced by randomly broken physical links (and simultaneous failing cyber nodes) by answering how many nodes will survive the cascade with a newly defined node yield metric. Specifically, we construct a framework to establish self-consistent equations of node yield through an auxiliary graph, without requiring the exact network topology. Then two algorithms are proposed to numerically calculate node yield for interdependent networks with arbitrary degree distributions. For random graph with Poisson degree distributions, we prove the existence of a critical initial edge disconnecting probability ϕ_{cr} under which an edge-induced cascade will result in dissolving the network topology, derive the closed form solution for ϕ_{cr}, and find that ϕ_{cr} increases sub-linearly with the mean degree of the physical network.**

I. Introduction

Internet of Things (IoT) is envisioned as a future paradigm that connects numerous physical devices, *i.e.*, "things", to the cyber world, *i.e.*, the Internet, creating an intelligent ecosystem that enables smart home, factory automation, intelligent transportation, and so on [1]. In such a system-of-systems, sensing and actuation become a *utility* [2], just like electricity and water, that is accessible by various *applications*, such as remote medicine and health care supported by home monitoring. Though the underlying platforms can be different and complicated, the nature of IoT systems is a networked *application* built upon networked *utility*, creating a strongly coupled cyber-physical system (CPS) [3]–[5]. For instance, in a mobile social network (MSN), smartphones can be connected by device-to-device (D2D) communication links as utility/physical nodes, and upon that the application/cyber network is composed of users connected by social interactions.

Along with these complex networks and communications, the intelligence of IoT systems is enabled by mutual connections between application and utility, through real-time communication and control. However, such close coupling introduces complex interdependence between cyber and physical domains, adding to the vulnerability of IoT systems [2]. On one hand, connection to the Internet that enables remote control, also surrenders IoT systems to malware [6] and cyber attacks [7], [8]. More importantly, because of the interdependence, faults triggered by a single incident in one domain, *e.g.*, a broken communication link or a hacked smart device, can propagate across both the cyber and physical domains, causing a chain of reactions, which is referred to as a *cascade-of-failures* in CPS [5], [9]. In IoT systems, such phenomena of cascade-of-failures can be especially detrimental since the actuators (physical nodes) can directly impact human lives. For example, a hacked smart home device (usually with weak security measures [7]), *e.g.*, a malfunctioning oven, is much more dangerous than a hacked computer that leaks personal information. To make things worse, the impact of cascade-of-failures can be even exacerbated by the massive scale of IoT systems [2], [10], as evidenced by the 2003 country-wide blackout in Italy [11]. Considering the severe impact of cascades in the physical world, it is crucial to understand the structural capacity of an IoT system in resisting cascades-of-failures, that is, the resilience in IoT systems with intrinsic characters of as interdependent networks.

Resilience of interdependent networks against random or correlated cascading failures is not a brand new topic, and has been addressed from two main aspects: the outcome after a cascade, and the critical condition of the system. The former reveals the impact of a cascade, as well as the expected replenishment/replacement workload. To this end, the remaining fraction of functional nodes after a cascade has been studied under random node failures [5], [12]. In terms of system restoration, resilience of a smart grid system has also been quantified by the control effort to steer the system back to normal operation [13]. The latter aspect examines the threshold behavior of interdependent networks, which provides important guidelines to the design of such systems. For example, Buldyrev *et.al.* found a critical average node degree below which an interdependent network will eventually collapse under random node failures.

The root causes of a cascade-of-failures can be attributed to cyber/physical node functions with respect to communication links, data acquisition, and reporting, *etc.*, while the *edge*, that

This work is partially supported by NSF CNS-1526152 and ARO W911NF-15-2-0102.

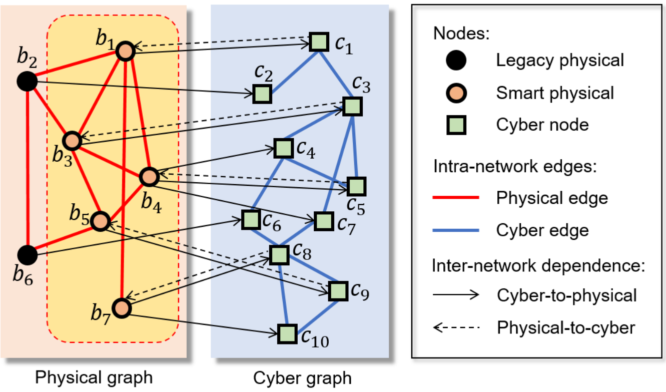


Fig. 1. An IoT system is modeled as an interdependent network $(\mathcal{G}_p, \mathcal{G}_c, \mathcal{E}_{c\to p}, \mathcal{E}_{p\to c})$. Direction of a cross-domain edge indicates the support/control relationship. For instance, cyber-to-physical edge $e(b_1 \to c_1) \in \mathcal{E}_{c\to p}$ (solid arrow) implies physical node b_1 *supports* cyber node c_1, so c_1 is *dependent* on b_1; physical-to-cyber edge $e(c_1 \to b_1) \in \mathcal{E}_{p\to c}$ (dashed arrow) indicates that c_1 *controls* b_1, so b_1 is *dependent* on c_1 as well.

is the connection between a node-pair, could be the consequence of any one of them or combination of multiple failures. Therefore, *broken links* in an IoT system are not only much more visible than individual failing nodes, but also indicate much more impacts in a networking perspective. The grand challenge is that the primary network modeling approach, graph theory, offers comprehensive results on networks with node failures, which can be random or targeted [4], [5], [9], [12]. The edge and node jointly-induced cascades, albeit as prevalent in IoT systems, have not been discussed in the context of interdependent networks. Links, especially those in the physical domain, are as vulnerable as (if not more than) nodes, so that link breakage/impairment constitutes a major cause of cascades in IoT systems: on one hand, many IoT applications rely on unstable wireless communication as their physical links and consequently suffer from random link breakages, *e.g.* D2D-based MSN and smart home devices connected by IEEE 802.11ah WiFi-HaLow [10]; on the other hand, wired utility links, such as power lines in smart grids, are under-guarded and exposed to vandalism. Though edge-induced cascades have been discussed in a single network context, *e.g.*, power grids [14] and scale-free networks [15], these results do not extend to IoT systems due to the complex interdependence. Motivated by the importance and lack of study, this paper addresses the *resilience problem* in IoT systems. Specifically, we aim to find:

(i) *residual node ratio*: how many nodes will survive an edge or jointly-induced cascade-of-failures?

(ii) *critical condition*: what is the minimum intensity of initial random failures to fully collapse an IoT system?

The rest of this paper is organized as follows. We introduce concept, system model and metrics in Sec. II to formulate the resilience problem of IoT systems. Then in Sec. III, an analytical framework is established to examine the expected residual node ratios of a generic IoT system under an edge or jointly-induced cascade. With the proposed framework, theoretical and numerical solutions of node yield for IoT systems with arbitrary node degree distributions are provided in Sec. IV. The critical initial disconnecting probability is studied with theoretical analysis and simulation in Sec. V. Finally, the paper is concluded in Sec. VI.

II. Resilience Problem in IoT Systems

In this section, we elaborate the resilience concept of IoT systems, and then briefly introduce our approach, the interdependent network model, triggering incidents, residual process and metrics to address the resilience problem.

A. What is Resilience in the IoT Context?

Resilience of a system measures its capability to maintain functions and structure in the face of internal and external change [16]. In the IoT context, it is the survivability of cyber and physical nodes against cascades induced by faults, failures and attacks. In a deterministic sense, resilience can be quantified by the expected response of an IoT system to a cascade, while in a probabilistic sense, it can be evaluated by the intensity of random failures that the system can withhold, as enumerated in the aforementioned *resilience problem*. From the outcome and critical condition aspects, answers to this problem offer information on the resisting capacity of an existing IoT system against cascades, as well as the necessary redundancy level in designing a future IoT system. However, the resilience problem is challenging due to the massive scale, complex interdependence, and broad application scenarios of IoT systems. Consequently, extracting meaningful insights through experiments is both difficult and costly, while analysis measures are hindered by the limited topology information that a large IoT system can provide.

B. Our Approach toward the Resilience Problem

To answer the resilience problem of IoT systems, we establish an analytical framework detailed as follows.

- Develop a network model of IoT systems to characterize the complex interdependence across the cyber and physical domains, and a network residual process to capture the impact of a cross-domain cascade.
- Define metrics, node yield Y_n and critical initial disconnection probability ϕ_{cr}, to quantify the resilience of an IoT system against edge and jointly-induced cascades.
- Construct an auxiliary graph to establish self-consistent equations, and derive node yield Y_n as a function of initial disconnecting probability ϕ and node degree distributions.
- Propose algorithms to numerically calculate node yield value for networks with arbitrary degree distributions.
- Prove the the existence of ϕ_{cr} in IoT systems with Poisson degree distributions with closed-form solutions.

C. Interdependent Network Model of an IoT System

Consider an IoT system that can be described as an interdependent network $(\mathcal{G}_p, \mathcal{G}_c, \mathcal{E}_{c\to p}, \mathcal{E}_{p\to c})$, illustrated by a simple example in Fig. 1. In this tuple, $\mathcal{G}_p(\mathcal{P}, \mathcal{E}_p)$ denotes the physical network that abstracts links between physical nodes (utility entities) in set $\mathcal{P} = \{b_1, \ldots, b_{n_p}\}$, while $\mathcal{G}_c(\mathcal{C}, \mathcal{E}_c)$ denotes the cyber network that describes connections between cyber nodes (application instances) in set $\mathcal{C} = \{c_1, \ldots, c_{n_c}\}$. Let $\{P_p(k)\}_{k=1}^{d_{max}(\mathcal{G}_p)}$ (respectively, $\{P_c(k)\}_{k=1}^{d_{max}(\mathcal{G}_c)}$) denote the node degree distribution of physical graph $\mathcal{G}_p$ (cyber graph $\mathcal{G}_c$), where $P_p(k)$ ($P_c(k)$) is the probability that a randomly selected physical (cyber) node is of degree k in graph $\mathcal{G}_p$ ($\mathcal{G}_c$).

The interdependent relationship between the physical and cyber domain of an IoT system is described by sets $\mathcal{E}_{c\to p}$ and $\mathcal{E}_{p\to c}$, that contain *directed* cross-domain edges. We adopt the 'one-to-multiple' support assumption in [5], and modify its 'one-to-one' control assumption to 'none/one-to-one', to allow modeling of legacy physical nodes, that only provide information support to applications, but maintain an isolated control. Specifically, one physical node can support multiple cyber nodes, while each 'smart' (non-legacy) physical node can only be controlled by one of its supported cyber nodes. In other words, for any physical node $b \in \mathcal{P}$:

a) There exists at most one cyber node $Ct(b) \in \mathcal{C}$ that can *control* physical node b (and hence b depends on $Ct(b)$), described by the directed edge $e\left(Ct(b) \to b\right) \in \mathcal{E}_{p\to c}$. We denote $Ct(b) = \varnothing$ if b is a legacy physical node that can not be controlled by any cyber node.

b) There exists a non-empty set $Sp(b) \subset \mathcal{C}$, containing all the cyber nodes that are supported by (hence *dependent on*) physical node b. Then for any cyber node $c_j \in Sp(b)$, there is a directed edge $e(b \to c_j) \in \mathcal{E}_{p\to c}$. Further, the number of cyber nodes $|Sp(b)|$ that a randomly chosen physical node $b \in \mathcal{P}$ supports follows a binomial distribution $\mathbf{B}(n_c, \frac{1}{n_p})$.

c) If $Ct(b) \neq \varnothing$, which means b is a smart physical node, then its controller $Ct(b)$ is chosen uniformly at random from its supported cyber nodes, *i.e.*, $Ct(b) \in Sp(b) \subset \mathcal{C}$.

Let $\mathcal{P}_s = \{b \in \mathcal{P} | Ct(b) \neq \varnothing\}$ denote the set of smart physical nodes, and $\alpha = \frac{\mathcal{P}_s}{\mathcal{P}}$ is referred to as the *adoption ratio* of the IoT system. Then, the system of interest, or more specifically the interdependent network $(\mathcal{G}_p, \mathcal{G}_c, \mathcal{E}_{c\to p}, \mathcal{E}_{p\to c})$, is characterized by a set of parameters, that is, the adoption ratio α, size n_p and degree distribution $\{P_p(k)\}_k$ of physical graph $\mathcal{G}_p$, and that (n_c and $\{P_c(k)\}_k$) of cyber graph $\mathcal{G}_c$.

D. Triggering Incident and the Cascade Process

Let time t proceed in discrete steps $\mathcal{T} = \{0, 1, \ldots\}$. Without loss of generality, let the triggering incident take place at time $t = 0$, when each physical edge in $\mathcal{E}_p$ disconnects with probability $\phi \in (0, 1)$, and each cyber node in $\mathcal{C}$ crashes with probability $\kappa\phi$, where $\kappa \in [0, 1]$. We call this triggering incident the *joint ϕ-edge and $\kappa\phi$-node failure*. Particularly, $\kappa = 0$ corresponds to the physical link breakage case, which we refer to as a `Type-1` scenario, while $\kappa > 0$ corresponds to a joint-failure case, referred to as the `Type-2` scenario. As a result of the initial failure, a set $\mathcal{E}_{fail}$ of physical links and set $\mathcal{C}_{fail}$ of cyber nodes are removed from the system at time $t = 0$, with expected values $\mathbb{E}(|\mathcal{E}_{fail}|) = \phi|\mathcal{E}_p|$ and $\mathbb{E}(|\mathcal{C}_{fail}|) = \kappa\phi n_c$ respectively.

Right after the initial failure, a sequence of alternating node/edge removal, *i.e.*, a *cascade*-of-failures, begin to unfold as time proceeds. Following a similar mechanism detailed in [5], we examine the residual physical network $\mathcal{G}_p(\mathcal{P}_t)$ in the first half of a time slot (odd steps), and the residual cyber network $\mathcal{G}_c(\mathcal{C}_t)$ in the second half (even steps). Note that $\mathcal{P}_t \subset \mathcal{P}$ and $\mathcal{C}_t \subset \mathcal{C}$ are time-decreasing sets of functional nodes at time t. At odd (respectively, even) steps, any physical (cyber) node is deemed as *dysfunctional* and removed, if it does not belong to the largest connected component (LCC) of the current remaining physical graph $\mathcal{G}_p(\mathcal{P}_t)$ (remaining cyber graph $\mathcal{G}_c(\mathcal{C}_t)$), or the cyber (physical) node it depends on was removed in the previous step. The removal of dysfunctional physical (respectively, cyber) nodes then results in the removal of all of its physical and support edges in $\mathcal{E}_p$ and $\mathcal{E}_{c\to p}$ (cyber and control edges in $\mathcal{E}_c$ and $\mathcal{E}_{p\to c}$). Fig. 2 illustrates an example of this cascade-of-failures process in the IoT system, whose network structure was shown in Fig. 1. To capture the evolution and impact of such cascades, we define a numerical random process that indicates the healthiness of the system.

Definition 1 (Physical/Cyber Residual Process)**.** *The residual physical node ratio R_t^p (respectively, residual cyber node ratio R_t^c) is defined as the proportion of physical (cyber) node that remains functional at time t, that is, $R_t^p := \frac{|\mathcal{P}_t|}{n_p}$ ($R_t^c := \frac{|\mathcal{C}_t|}{n_c}$). The resulting processes $\{R_t^p\}_t$ and $\{R_t^c\}_t$ are called physical and cyber residual processes respectively.*

Since the residual networks $\mathcal{G}_p(\mathcal{P}_t)$ and $\mathcal{G}_c(\mathcal{C}_t)$ are node-induced graphs of $\mathcal{G}_p$ and $\mathcal{G}_c$, random variables R_t^p and R_t^c both take value in $[0, 1]$, and the residual processes $\{R_t^p\}_t$ and $\{R_t^c\}_t$ are non-increasing in time t.

E. Metrics and Problem Formulation

The resilience problem focuses on the final *outcome* and *critical condition* of the network under cascades, that is, *will the network collapse*? If not, *how many will remain functional*? To answer these questions, we define the following metrics.

Definition 2 (Node Yield[1])**.** *Given a physical residual process $\{R_t^p\}_{t\in\mathcal{T}}$ of an IoT system $(\mathcal{G}_p, \mathcal{G}_c, \mathcal{E}_{c\to p}, \mathcal{E}_{p\to c})$, node yield Y_n is defined as the expected minimum residual physical node ratio over time, that is,*

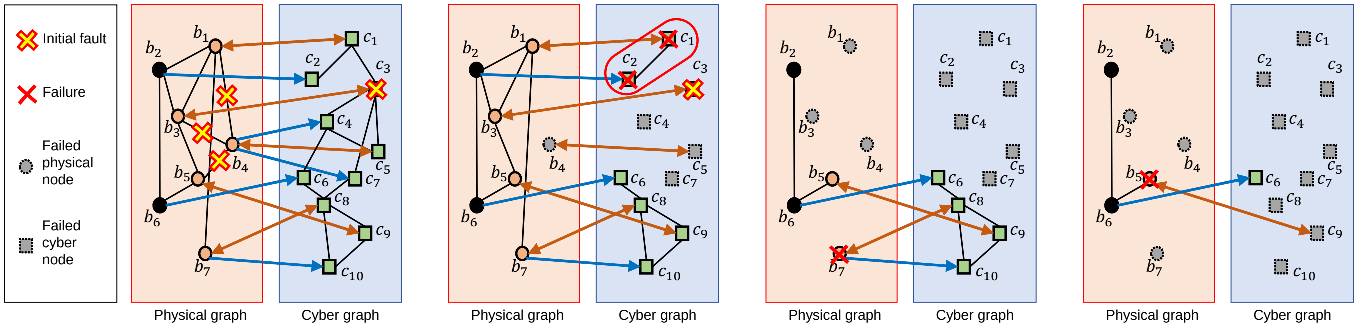
$$Y_n := \min_{t\in\mathcal{T}} \mathbb{E}(R_t^p) = \lim_{t\to\infty} \mathbb{E}(R_t^p). \tag{1}$$

Node yield Y_n illustrates the worst-case impact of a cascade-of-failures on an IoT system given long enough time. Viewing node yield as a function of the initial disconnecting probability ϕ, we identify the critical condition ϕ_{cr} upon which the interdependent network will eventually collapse.

Definition 3. *Let $Y_n(\phi)$ denote the value of node yield as a function of the physical edge disconnecting probability ϕ. Then, the critical disconnection probability ϕ_{cr} is defined as the minimum ϕ that triggers total network fragmentation, i.e.,*

$$\phi_{cr} := \max\{0 \leq \phi \leq 1 \mid Y_n(\phi) > 0\}. \tag{2}$$

[1] The name, node yield, is inspired by the *demand yield* defined in the smart grid context [17], which represents the portion of serviceable electricity demand after cascades.



(a) Step 1: Removal in $\mathcal{G}_p$ and $\mathcal{E}_{c\to p}$ ($t=1$)

(b) Step 2: $\mathcal{G}_c$ and $\mathcal{E}_{p\to c}$ ($t=1$)

(c) Step 3: $\mathcal{G}_p$ and $\mathcal{E}_{c\to p}$ ($t=2$)

(d) Step 4: $\mathcal{G}_c$ and $\mathcal{E}_{p\to c}$ ($t=2$)

Fig. 2. Step-by-step illustration of cascading failures (Type-2) in an interdependent network: During $t=1$, (a) disconnected physical edges $\{e(b_1,b_4), e(b_3,b_4), e(b_4,b_5)\}$ are removed, resulting in the removal of node b_4 and all of its supporting edges in $\mathcal{E}_{c\to p}$; (b) then in $\mathcal{G}_c$, node c_3 is removed due to initial failure, $\{c_4,c_5,c_7\}$ for losing support, and $\{c_1,c_2\}$ for disconnection to the LCC, together with their control edges in $\mathcal{E}_{p\to c}$. Current residual ratio $R_1^p=\frac{6}{7}$, $R_1^c=\frac{4}{10}$. Then similarly in $t=2$, (c) physical nodes $\{b_1,b_3\}$ are removed due to lost of control edges, and b_7 for not in LCC; (d) after similar operations, cyber graph $\mathcal{G}_c$ dissolves and $R_2^c=0$. Eventually, only legacy physical nodes b_2 and b_6 are functional, so node yield becomes $Y_n=\frac{2}{7}$.

Critical condition ϕ_{cr} identifies the worst initial failure that an interdependent network can barely survive, so that at least $\phi_{cr}|\mathcal{E}_p|$ amount of physical edges will need to be removed to collapse the network. With the defined metrics, the resilience problem in IoT systems now translates to the following mathematical questions. Given an IoT network with adoption ratio α, composed of physical graph $\mathcal{G}_p$ of size n_p and degree distribution $\{P_p(k)\}_k$, and cyber graph $\mathcal{G}_c$ of size n_c and degree distribution $\{P_c(k)\}_k$: What is the node yield Y_n under a cascade induced by the joint ϕ-edge $\kappa\phi$-node failure? Is there a critical initial disconnecting probability ϕ_{cr} such that node yield $Y_n=0$?

III. Analysis Framework For Residual Processes

In order to answer the first question of the resilience problem, *i.e.*, the outcome of a cascade, we first analyze the process of residual physical node ratios $\{R_t^p\}_t$, because node yield is the minimum expected physical residual that does not change over time any more. On the residual fraction, Huang *et al.* employed percolation theory to describe cascading failures induced by random physical node failures (referred to as Type-0 scenario), for scale-free interdependent networks of infinite size [5]. However, their model and solution do not apply to edge-induced cascades (Type-1 scenario), or the more complicated jointly-induced cascades (Type-2 scenario). To overcome this challenge, we introduce a framework that maps Type-1 and Type-2 scenarios to equivalent Type-0 scenarios, and then develop self-consistent equations on the residual processes so that node yield can be analyzed later.

A. Mapping of the Triggering Incident

The main idea of the mapping method is to construct an auxiliary interdependent network $(\tilde{\mathcal{G}}_p,\mathcal{G}_c)$, such that the residual process of the original network $(\mathcal{G}_p,\mathcal{G}_c)$ under an edge or jointly-induced cascade, is equivalent to that of the auxiliary graph $(\tilde{\mathcal{G}}_p,\mathcal{G}_c)$ under a node-induced cascade. Specifically, this is done by matching the initial impact (removal) between the two scenarios at time $t=0$. In this section, we assume that edge disconnections occur and modify only the physical graph, *i.e.* random physical link breakages, so that the structure of the auxiliary and original cyber graphs remain equal to $\mathcal{G}_c$. But we note here that initial cyber link breakages can similarly be analyzed by exchanging subscripts $()_p$ and $()_c$.

1) Type-0 scenario as a primer: Consider a cascade induced by random physical node failures in the auxiliary interdependent network $(\tilde{\mathcal{G}}_p,\mathcal{G}_c)$, whose construction will be detailed in the next subsection. Let $\tilde{\phi}_p$ denote the node failing probability/ratio in the physical graph $\tilde{\mathcal{G}}_p(\mathcal{P},\tilde{\mathcal{E}}_p)$, and its degree distribution is characterized by $\{\tilde{P}_p(k)\}_k$.

After the random node removal in $\tilde{\mathcal{G}}_p$ at $t=0$, a fraction $(1-\tilde{\phi}_p)$ of the $|\tilde{\mathcal{P}}_p|$ physical nodes remain. These nodes may further fragment into disconnected components among which the fraction that still belongs to the LCC of $\tilde{\mathcal{G}}_p$ is given [12] as

$$\tilde{g}_p(\tilde{\phi}_p)=1-\tilde{G}_{p,1}\left(1-(1-\tilde{\phi}_p)(1-f_p)\right). \tag{3}$$

Here, $\tilde{G}_{p,1}(x):=\tilde{G}'_{p,0}(x)/\tilde{G}'_{p,0}(1)$ is a supplementary function, while $\tilde{G}'_{p,0}(x):=\frac{d}{dx}\tilde{G}_{p,0}(x)$ denotes the first-order derivative of the probability generating function (PGF)

$$\tilde{G}_{p,0}(x):=\sum_{k=0}^{\infty}\tilde{P}_p(k)x^k \tag{4}$$

of the degree distribution $\{\tilde{P}_p(k)\}_k$. Moreover, f_p is a variable that satisfies a transcendental (self-consistent) equation

$$f_p=\tilde{G}_{p,1}\left(1-(1-\tilde{\phi}_p)(1-f_p)\right). \tag{5}$$

Similar results apply to the cyber graph $\tilde{\mathcal{G}}_c$ after random cyber node removal with probability ϕ_c, and can be obtained by substituting the subscript $()_p$ with $()_c$ and omitting the tilde sign in Eq. (3)-(5). The remaining LCC fractions $\tilde{g}_p$ and g_c will be utilized in analyzing the expected residual physical/cyber node fractions, as discussed by the step-by-step measure in [5]. So, it is crucial to construct the auxiliary graph to match the impact of random edge and joint failures.

2) Construction of the Auxiliary Graph $(\tilde{\mathcal{G}}_p, \mathcal{G}_c)$*:* As indicated by Eq. (3)-(5), the key intermediate parameters in the residual process analysis are the node removal probability $\tilde{\phi}_p$ and the PGF $\tilde{G}_{p,0}(x)$. Therefore, for `Type-1` scenario, the goal of the construction is to match these parameters, that is, to find the corresponding $\tilde{\phi}_p$ and $\tilde{G}_{p,0}(x)$ in terms of the initial disconnecting probability ϕ and physical node degree distribution $\{P_p(k)\}_k$ of the original interdependent network.

Right after the random physical link/edge disconnection, the probability that a physical node $b_i \in \mathcal{P}$ is fully disconnected, *i.e.*, losing all of its physical edges, is $\phi^{d_p(b_i)}$. Then from the network's point-of-view, the expected fraction/ratio of physical nodes that are to be removed (due to edge disconnection) is

$$\tilde{\phi}_p = \sum_{k=0}^{\infty} P_p(k)\phi^k. \tag{6}$$

In addition, because of the random link breakages, the node degree distribution of the remaining graph becomes

$$P_{\phi,p}(k) = \sum_{j=k}^{\infty} P_p(j)\phi^{j-k}(1-\phi)^k, \tag{7}$$

with PGF $G_{\phi,p}(x) = \sum_{k=0}^{\infty} P_{\phi,p}(k)x^k$.

To match Eq. (7) against the node degree distribution of auxiliary graph $\tilde{\mathcal{G}}_p$ in `Type-0` scenario (random physical node failures), the PGF of the resulting degree distribution in the auxiliary graph $\tilde{\mathcal{G}}_p$ after initial removal of physical nodes should equal to $G_{\phi,p}(x)$. Then, we have

$$\tilde{G}_{p,0}\left(\tilde{\phi}_p + (1-\tilde{\phi}_p)x\right) = G_{\phi,p}(x) \tag{8}$$

from [12], where $\tilde{G}_{p,0}(x)$ denotes the PGF of the auxiliary graph $\tilde{\mathcal{G}}_p$ before initial node removal in `Type-0` scenario, and $\tilde{\phi}_p$ can be obtained from Eq. (6). Performing an inversion to Eq. (8) gives

$$\tilde{G}_{p,0}(x) = G_{\phi,p}\left(\frac{x-\tilde{\phi}_p}{1-\tilde{\phi}_p}\right). \tag{9}$$

Note that the set of physical nodes remain the same in the auxiliary physical graph $\tilde{G}_p$ and the original G_p, so do the cross-domain edges for interdependence, while the only difference is the degree distribution in the physical domain. For `Type-2` scenario, where random physical link breakages are accompanied by random cyber node failures, similar procedure can be applied to construct the auxiliary $\tilde{\mathcal{G}}_p$, since all the initial random edge disconnection occur in the physical graph $\mathcal{G}_p$. In fact, as we will show in the next subsection (Lemma 1), the two influences can be jointly considered in one auxiliary physical graph $\tilde{\mathcal{G}}_p$, such that derived self-consistent equations can apply to both `Type-1` and `Type-2` scenarios.

B. Self-consistent Equations of the Expected Network Residual

With auxiliary graph $(\tilde{\mathcal{G}}_p, \mathcal{G}_c)$ in which initial edge failures in `Type-1` and `Type-2` scenarios are transformed into an equivalent `Type-0` scenario, the network residual processes $\{R_t^p\}_t$ and $\{R_t^c\}_t$ (see Definition 1) can be analyzed through self-consistent equations.

Lemma 1 (Expected physical/cyber residual ratio)**.** *Denote* $x_t := \mathbb{E}(R_t^p)$ *and* $y_t := \mathbb{E}(R_t^c)$ *as the expected residual physical and cyber node ratios of the original IoT system* $(\mathcal{G}_p, \mathcal{G}_c)$ *(with adoption ratio* α*) at time* t*. Then, under a joint* ϕ*-edge and* $\kappa\phi$*-node failure,*

$$\begin{aligned} x_t &= x_t' \times \tilde{g}_p(x_t'), \text{ and} && (10) \\ y_t &= y_t' \times g_c(y_t'), && (11) \end{aligned}$$

where quantities x_t' *and* y_t' *satisfy*

$$\begin{cases} x_t' = (1-\tilde{\phi}_p)(1-\kappa\phi)\left[1-\alpha\left(1-g_c(y_{t-1}')\right)\right], \\ y_t' = (1-\tilde{\phi}_p)(1-\kappa\phi) \times \tilde{g}_p(x_t'), \end{cases} \tag{12}$$

in which the equivalent node removal probability $\tilde{\phi}_p$ *can be obtained from Eq.* (6)*; remaining LCC fractions* $\tilde{g}_p()$ *and* $g_c()$ *can be found in Eq.* (3)*.*

Lemma 1 can be proved with a similar step-by-step technique presented in [5, Sec. 5], to which interested readers are directed. Note that the physical meaning of x_t' and y_t' are the expected fractions of the *remaining* physical/cyber node after the last time step $t-1$, but not the *residual* fraction, because some of the remaining nodes may not be functional as they are not in the LCC.

In addition, consider `Type-2` scenario ($\kappa > 0$) in which physical edges break with probability ϕ and cyber nodes crash with probability $\kappa\phi$. After removing $\tilde{\phi}_p$ and $\kappa\phi$ fractions of nodes from $\tilde{\mathcal{G}}_p$ and $\mathcal{G}_c$, the fraction of nodes that are residues in *both* $\tilde{\mathcal{G}}_p$ and $\mathcal{G}_c$ becomes $\tilde{\phi}_p \times \kappa\phi$. As a result, discarding $\tilde{\phi}_p$ and $\kappa\phi$ fractions of nodes *separately* is equivalent to removing $(1-\tilde{\phi}_p)(1-\kappa\phi)$ fraction of nodes from *either* graph $\tilde{\mathcal{G}}_p$ or graph $\mathcal{G}_c$ alone. We assume that the removals occur in $\tilde{\mathcal{G}}_p$ to be consistence with `Type-1` scenario ($\kappa = 0$). Though the employed proof technique is similar with [5], it should be noted that [5] is restricted to a full adoption ($\alpha = 1$) case, where every physical node is controlled by a cyber node, while our model can be applied to scenarios that contain legacy manually-controlled physical nodes.

IV. Solution of Node Yield from Self-consistent Equations

Recall that node yield Y_n is defined as the expected steady state of physical residual process $\{R_t^p\}$, that is, $x_t = x_{t-1}$ in Lemma 1. The key challenge of obtaining Y_n from Lemma 1 lies in finding the solution to Eq. (12), that is tied closely to node degree distributions of the physical network $\mathcal{G}_p$ and the cyber network $\mathcal{G}_c$. Interdependent networks with power law degree distribution have been discussed in [5] for random physical node failures (`Type-0`). However, various application scenarios of IoT render an assortment of node degree distributions. To address this, we provide calculation measures of the node yield Y_n in this section, for interdependent networks with generic node degree distributions.

A. Poisson Degree Distribution

Random graph (Erdös-Rényi or ER graphs) has been identified to be useful in realizing network connectivity and resource distribution in IoT systems [18]. For instance, a D2D-based MSN on a conference was shown to follow Poisson node distributions [19], which corresponds to an ER graph. For this kind of networks, we have the following theorem.

Theorem 1. *If node degrees of physical graph $\mathcal{G}_p$ and cyber graph $\mathcal{G}_c$ follow Poisson distribution with mean $\bar{k}_p$ and $\bar{k}_c$, respectively, then the under joint ϕ-edge and $\kappa\phi$-node failure, the node yield Y_n of the system satisfies*

$$\begin{aligned} Y_n &= (1-\kappa\phi)\left(1-e^{-\bar{k}_p(1-\phi)}\right)\left(1-\alpha\exp\left\{-\bar{k}_c Y_n\right\}\right) \\ &\times\left(1-\exp\left\{-\frac{\bar{k}_p(1-\phi)}{1-\exp(-\bar{k}_p(1-\phi))}Y_n\right\}\right). \end{aligned} \tag{13}$$

Proof: Physical graph $\mathcal{G}_p$ has a Poisson degree distribution of $P_p(k)=\frac{e^{-\bar{k}_p}}{k!}(\bar{k}_p)^k$. Plugging $P_p(k)$ into Eq. (7), we obtain the degree distribution of $\mathcal{G}_p$ after the initial failure,

$$P_{\phi,p}(k) = \frac{e^{-\bar{k}_p}}{k!}\left(\frac{1-\phi}{\phi}\right)^k\sum_{j=k}^{\infty}\frac{1}{(j-k)!}(\bar{k}_p\phi)^j \tag{14}$$

$$= \frac{e^{-\bar{k}_p\phi}}{k!}\left(\bar{k}_p(1-\phi)\right)^k. \tag{15}$$

From Eq. (7) and its following explanation, the PGF of $\{P_{\phi,p}(k)\}_k$ can be restated as

$$G_{\phi,p}(x) = e^{\bar{k}_p(1-\phi)(x-1)}. \tag{16}$$

According to Eq. (6), the average fraction of physical node to be removed is $\tilde{\phi}_p = e^{-\bar{k}_p\phi}$. Combining this with Eq. (16), we can derive the PGF of the auxiliary graph $\tilde{\mathcal{G}}_p$ before the equivalent initial node removal, that is, $\tilde{G}_{p,0}(x)$, from Eq. (9). Subsequently, we have

$$\tilde{g}_p(x) = 1-\tilde{G}_{p,0}(1-x(1-f_p)) = 1-f_p, \tag{17}$$

since $\tilde{G}_{p,1}(x)=\tilde{G}'_{p,0}(x)/\tilde{G}'_{p,0}(1)$ and $f_p=\tilde{G}_{p,1}(1-x(1-f_p))=\exp(\frac{-\bar{k}_p(1-\phi)}{1-\exp(-\bar{k}_p(1-\phi))}x(1-f_p))$ by definition.

The cyber graph $\mathcal{G}_c$, on the other hand, has a degree distribution of $P_c(k)=\frac{(\bar{k}_c)^k}{k!}e^{-\bar{k}_c}$ and a PGF of $G_{c,0}(x)=e^{\bar{k}_c(x-1)}$. Hence, we obtain

$$g_c(y) = 1-G_{c,0}(1-y(1-f_c)) = 1-f_c, \tag{18}$$

with f_c satisfying $f_c=G_{c,1}(1-y(1-f_c))=e^{-\bar{k}_c y(1-f_c)}$.

At steady state, denote $x^* := x'_t = x'_{t-1}$ and $y^* := y'_t = y'_{t-1}$ to indicate that the expected remaining fractions become constant. Then, we plug Eq. (17)-(18) into Lemma 1 and re-evaluate the node yield as

$$\begin{aligned} Y_n &= (1-\tilde{\phi}_p)(1-\kappa\phi)\left[1-\alpha(1-g_c(y^*)\right]\times\tilde{g}_p(x^*) \qquad (19) \\ &= (1-e^{-\bar{k}_p(1-\phi)})(1-\kappa\phi)(1-\alpha[\exp\{-\bar{k}_c y^*(1-f_c)\}]) \\ &\times\left(1-\exp\left\{-\frac{\bar{k}_p(1-\phi)}{1-\exp\{-\bar{k}_p(1-\phi)\}}x^*(1-f_p)\right\}\right). \end{aligned}$$

To proceed, we assume that adoption ratio α is large (near one). This assumption is reasonable in future IoT scenarios like smart grid and intelligent transportation systems, where many physical resources are controlled by cyber entities/controllers. Then, Eq. (13) can be acquired by approximating the node yield given in Eq. (19) with $Y_n \approx (1-e^{-\bar{k}_p(1-\phi)})(1-\kappa\phi)(1-f_p)(1-f_c)$. ∎

Theorem 1 gives a closed-form result on node yield in networks with Poisson degree distributions, that can then be solved graphically or via the bisection method. It is known that Binomial degree distribution converges to Poisson for large number of vertices [20], so we validate our theoretical analysis in Theorem 1 in a system whose physical and cyber degrees follow $\mathbf{B}(n_p,\frac{\bar{k}_p}{n_p})$ and $\mathbf{B}(n_c,\frac{\bar{k}_c}{n_c})$ respectively. Unless specified otherwise, we generate ER networks with $n_p = n_c = 5000$ nodes, set the mean physical and cyber degrees to $\bar{k}_p=\bar{k}_c=10$, and employ the adoption ratio of $\alpha=1$. Each of the presented numerical result is executed in `Python` over 5×10^3 network realizations.

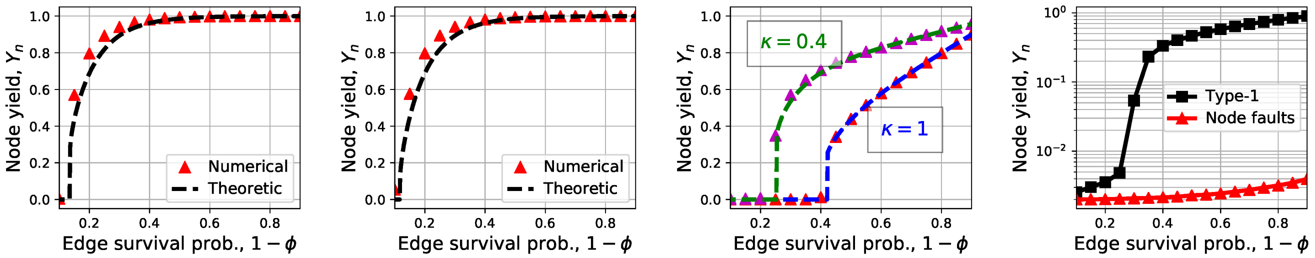
We plot in Fig. 3.(a) the node yield Y_n versus physical edge survival ratio $1-\phi$ in `Type-1` ($\kappa=0$) scenario. The numerical simulation result is shown with red triangle markers, while dashed black lines represent analytical result in Eq. (23), which is obtained via the *bisection method* [21, Alg. 4.1]. We observe that the former agrees with the latter, as indicated by Theorem 1. The validity is preserved for $0<\alpha<1$, as implied by the matching plots in Fig. 3.(b) even when the adoption ratio α is reduced to 0.2. Moreover, high similarity between Fig. 3.(a) and (b) reveals that the impact of α to node yield is negligible in `Type-1` scenarios. For `Type-2` scenario, we employ different κ values in Fig. 3.(c): $\kappa=1$ and $\kappa=0.4$, and observe an agreement between the analytical and numerical simulations. In addition, as κ decreases, the result for `Type-2` scenario converges to the node yield of `Type-1` scenario in Fig. 3.(a), that is, a special case of $\kappa=0$.

To visualize the importance comparison between physical edges and cyber nodes, we compare a 'pure' cyber node failure (red triangle markers), discussed in [9], to `Type-1` scenario ('pure' physical edge disconnection, black square markers) in Fig. 3.(d). Observe that the resulting node yield Y_n is smaller upon cyber node failures, indicating IoT is more vulnerable against cyber node failures due to cyber attacks or software crashes. This is because random cyber node failures will result in a lower average degree (and generally low degrees among nodes) in the physical graph, right after the removal of initially failed cyber nodes, which can be observed by examining quantity $\{P_{\phi,p}(k)\}_k$. Therefore, a practical guidance for IoT protection is that cyber nodes should be safe-guarded with more resource to sustain a robust IoT service.

B. Generic Degree Distribution

In a more general sense, the physical and cyber node degrees of an IoT system do not always follow distributions with nice properties, *e.g.*, Poisson or power law. Rather, they can be quite spontaneous. For these cases, we propose two iterative algorithms to solve node yield Y_n from Eq. (10) - (12).

A key to numerically solving node yield from Lemma 1 is to find the steady fraction of the remaining (not residual)



(a) `Type-1` with $\alpha = 1$. (b) `Type-1` with $\alpha = 0.2$. (c) `Type-2` initial fault. (d) `Type-1` vs node removal [9].

Fig. 3. Validation of Theorem 1: Theoretical results of node yield Y_n obtained from Theorem 1. match with that obtained from numerical simulations in a cyber-physical networks ($n_p = n_c = 5000$ nodes) with Binomial degree distributions ($\bar{k}_p = \bar{k}_c = 10$).

Algorithm 1 Calculation of node yield, Y_n

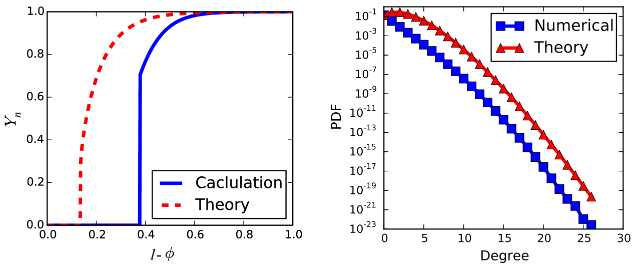
```
 1: procedure NODE-YIELD($\phi$)
 2:     $a \leftarrow 0,\ b \leftarrow 1$                         ▷ initial condition
 3:     repeat
 4:         Calculate $g(a) \leftarrow x^*(a) - a$
 5:         Calculate $c \leftarrow \frac{a+b}{2}$ and $g(c) \leftarrow x^*(c) - c$
 6:         if $sgn(g(c)) = sgn(g(a))$ then $a \leftarrow c$
 7:         else $b \leftarrow c$
 8:         end if
 9:     until convergence
10:     $x^* \leftarrow x^*(c)$
11: return $x^* \times$ GP-CALC($x^*$)         ▷ Outputs $Y_n = x^* \tilde{g}_p(x^*)$
12: end procedure
13: function $x^*(a)$
14:     Calculate $p_p$ using Eq. (6)
15:     $y' \leftarrow p_p \times$ GP-CALC($a$)
16:     return $p_p \times (1 - \alpha[1 - $GC-CALC$(y')])$
17: end function
```

Algorithm 2 Calculation of $\tilde{g}_p(x^*)$

```
 1: procedure GP-CALC($x^*$)
 2:     $a \leftarrow 0,\ b \leftarrow 1$                         ▷ initial condition
 3:     repeat
 4:         Calculate $g(a) \leftarrow f_p(a, x^*) - a$
 5:         Calculate $c \leftarrow \frac{a+b}{2}$ and $g(c) \leftarrow f_p(c, x^*) - c$
 6:         if $sgn(g(c)) = sgn(g(a))$ then $a \leftarrow c$
 7:         else $b \leftarrow c$
 8:         end if
 9:     until convergence
10: return $1 - c$             ▷ Returns $\tilde{g}_p(x^*)$ satisfying Eq. (3)-(5)
11: end procedure
12: function $f_p(a, x^*)$
13:     Calculate $\tilde{x} \leftarrow 1 - x^*(1 - a)$
14:     return $\frac{\tilde{G}_{p,1}(\tilde{x}+h)-\tilde{G}_{p,1}(\tilde{x}-h)}{\tilde{G}_{p,1}(1+h)-\tilde{G}_{p,1}(1-h)}$
15: end function
16: function $\tilde{G}_{p,1}(\tilde{x})$
17:     Calculate $P_{\phi,p}(k)$ for all $k$ using Eq. (7)
18:     return $\sum_{k=0}^{\infty} P_{\phi,p}(k)(\frac{\tilde{x}}{1-\phi_p} + (1 - \frac{1}{1-\phi_p}))^k$
19: end function
```

fraction of physical nodes x^* and that of the cyber nodes y^*. This imposes two challenges: (i) determining x^* that satisfies the self-consistent equation in Eq. (12), and (ii) finding the LCC fractions $\tilde{g}_p$ and g_c on the right sides of Eq. (12), that satisfy another self-consistent equation, Eq. (5). To find these values simultaneously, we apply a *two-step process* as follows. At the first (higher) level, we solve x^* in Eq. (12) by applying Algorithm 1. Since x^*, $\tilde{g}_p$, and g_c all take value in $[0, 1]$, we can find their respective values using the bisection method [21], which essentially performs a binary search over a continuous range $[0, 1]$ (see line 2-9 in Algorithm 1) until either the number of iterations is large enough or the solution is close enough to the convergence point.

For every first-level iteration, we solve $\tilde{g}_p$ and g_c at the second (lower) level. Specifically, $\tilde{g}_p$ is obtained by applying Algorithm 2. In Algorithm 2, line 2-9 is the bisection algorithm, line 12-15 applies the *finite difference method* [22] to calculate the derivative $\tilde{G}_{p,1}(x) = \frac{\tilde{G}'_{p,0}(x)}{\tilde{G}'_{p,0}(1)}$, while line 16-19 employs our mapping described by Eq. (7)-(9). Quantity g_c (as called by GC-CALC in line 16 of Algorithm 1) can be found by re-using Algorithm 2 after substituting subscript $()_p$ with $()_c$, omitting the tilde symbol, and directly applying the degree distribution of $\mathcal{G}_c$ into Eq. (4).



(a) Calculation of node yield Y_n (b) Degree distribution $P_{\phi,p}(k)$

Fig. 4. Evaluation of the proposed Algorithm 1 and 2 in Erdös-Rényi graphs.

To evaluate the numerical scheme, we compare the calculated node yield (blue solid line) from Algorithm 1 to the analysis in Eq. (13) (red dashed line) in Fig. 4.(a). We observe the existence of a gap between the numerical calculation and theoretic analysis, which can be attributed to two main reasons. Firstly, numerical calculation of the PDF of the physical node degree distribution right after the physical edge removal, *i.e.*,

$P_{\phi,p}(k)$, relies on the *infinite sum* of the degree, while empirical degree, however, is upper-bounded. Thus, the numerical result for the sum as shown in Fig. 4.(b), will always be underestimated. Secondly, the centered difference method used in Algorithm 2 to approximate derivative $G_{p,1}(x) = \frac{G'_{p,0}(x)}{G'_{p,0}(1)}$ also introduces deviation, especially when x is small. Note that, despite the numerical gap, Algorithm 1 and 2 provide a crude estimate of the node yield Y_n.

V. Resilience of IoT through Critical Disconnecting Probability ϕ_{cr}

Apart from the outcome aspect that is addressed in the previous two sections, resilience is also a measure of a network's intrinsic capability to resist faults and attacks, as described by the second half of the resilience problem. In other words, *what is the worst case attack an IoT system can withhold*? For instance, resilience of a simple network is quantified by its connectivity [23], *i.e.*, the minimum number of edges to be removed before the network becomes disconnected. In a similar spirit, we expand the existing notion of connectivity-based resilience to interdependent IoT systems, with respect to the intensity of the triggering incident, *i.e.* the edge disconnecting probability ϕ. Particularly, we examine the existence of a critical condition ϕ_{cr} in interdependent networks with Poisson degree distributions (ER graphs), through theoretical analysis and numerical simulations.

A. Theoretical Analysis on Critical Disconnecting Ratio ϕ_{cr}

For interdependent network with Poisson degree distribution in both cyber and physical domains, we prove the existence of such a critical condition ϕ_{cr} upon which an IoT system can fully fragment into isolated nodes and collapse. Further, we provide a closed-form solution to ϕ_{cr}, *i.e.*, the critical initial disconnecting probability, with respect to structural properties of the interdependent network.

Theorem 2. *Consider an interdependent network* $(\mathcal{G}_p, \mathcal{G}_c)$ *with Poisson physical degree distributions of mean* $\bar{k}_p$*, and an adoption ratio of* $\alpha = 1$*. The critical disconnection probability* ϕ_{cr} *can be approximated by*

$$\phi_{cr} \approx \begin{cases} 1 - \frac{1.59362}{\bar{k}_p}, & \textit{under } \texttt{Type-1} \textit{ fault,} \\ 1 - \frac{\kappa+1}{\kappa+\bar{k}_p}, & \textit{under } \texttt{Type-2} \textit{ fault.} \end{cases} \tag{20}$$

Proof: We start by considering `Type-1` scenario. In this case, solving ϕ_{cr} is equivalent to finding the smallest edge survival ratio $\gamma = 1 - \phi_{cr}$ that results in a non-zero node yield Y_n, where Y_n satisfies Eq. (13). To this end, we apply the following two-step approach.

(Step 1) By assuming that γ is fixed, we find Y_n such that the left-hand side of Eq. (13) has the same gradient as the right-hand side. In this so called *gradient condition*, the following equation holds.

$$\begin{aligned} \frac{d}{dY_n} Y_n \quad &= \quad \frac{d}{dY_n} \left[\left(1 - e^{-\bar{k}_p\gamma}\right) \left(1 - \exp\left\{-\bar{k}_c Y_n\right\}\right) \right. \\ &\quad \left. \times \left(1 - \exp\left\{-\frac{\bar{k}_p\gamma}{1 - \exp(-\bar{k}_p\gamma)} Y_n\right\}\right)\right]. \end{aligned} \tag{21}$$

To proceed, a first-order Taylor series approximation $e^{-f(Y_n)} \approx 1 - f(Y_n)$ [24] is applied to Eq. (21) such that the gradient condition in Eq. (21) becomes

$$1 = \frac{(1 - e^{-\bar{k}_p\gamma})\bar{k}_p\bar{k}_c\gamma}{1 - \exp\{-\bar{k}_p\gamma\}} \times 2Y_n. \tag{22}$$

Then, solution to Eq. (22) can be found as

$$Y_n = (2\bar{k}_c\bar{k}_p\gamma)^{-1}. \tag{23}$$

(Step 2) Next, given Y_n in Eq. (23) above, we find the critical ratio γ_{cr}. To illustrate how this is done, we present Fig. 5.(a), where the curve is plotted for different initial ratios, $\phi_1 < \phi_{cr} < \phi_2$. Note that there can be several values of ϕ's with their corresponding Y_n's that satisfy the gradient condition. However, there is only one, $\phi_{cr} = 1 - \gamma_{cr}$, that satisfies the *critical condition* in which the line and curve intersects non-trivially (i.e. other than at origin) only once. This critical solution can be obtained by plugging Eq. (23) into Eq. (13) and re-applying the Taylor series approximation. We obtain $\frac{1}{2\bar{k}_c\bar{k}_p\gamma_{cr}} = \bar{k}_p\gamma_{cr}\left(\frac{\bar{k}_c}{2\bar{k}_c\bar{k}_p\gamma}\right) \times \left(\frac{\bar{k}_p\gamma_{cr}}{1-\exp\{-\bar{k}_p\gamma_{cr}\}} \times \frac{1}{2\bar{k}_c\bar{k}_p\gamma_{cr}}\right)$.

After re-arranging and variable eliminations,

$$\bar{k}_p\gamma_{cr} = 2\left(1 - \exp\{-\bar{k}_p\gamma_{cr}\}\right). \tag{24}$$

Numerical evaluations [25] show that Eq. (24) has two solutions: $\bar{k}_p\gamma_{cr} = 0$ and $\bar{k}_p\gamma_{cr} = 1.59362$. Taking the non-trivial solution (the latter) completes the proof for `Type-1` scenario.

For cyber-physical networks in `Type-2` scenario, we re-employ the Steps 1 and 2 above to the self-consistent equation Eq. (13), and obtain

$$(1 - \exp\{-\bar{k}_p\gamma_{cr}\}) = \bar{k}_p\gamma_{cr}(1 - \kappa(1 - \gamma_{cr})). \tag{25}$$

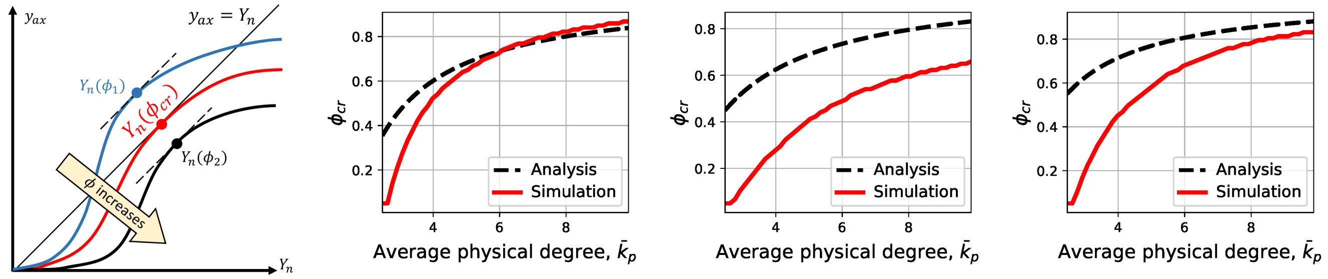
By applying a second-order Taylor approximation $e^{-f(\gamma_{cr})} \approx 1 - f(\gamma_{cr}) + \frac{(-f(\gamma_{cr}))^2}{2!}$ to the left-hand side of Eq. (25),

$$2\left(\bar{k}_p\gamma_{cr} - \frac{\bar{k}_p^2\gamma_{cr}^2}{2}\right) = \bar{k}_p\gamma_{cr}\left(1 - \kappa(1 - \gamma_{cr})\right). \tag{26}$$

Finally, the second line of Eq. (20) can be acquired after re-arranging Eq. (26) and plugging the obtained critical residual ratio γ_{cr} into $\phi_{cr} = 1 - \gamma_{cr}$. ■

B. Numerical Simulation

To validate the analytical critical initial disconnecting probability ϕ_{cr} obtained from Eq. (20), we first consider `Type-1` scenario and re-use the simulation parameters in the previous section. In Fig. 5.(b), the analytical result (dashed black line) is compared to the numerical solution (solid red line) that searches ϕ_{cr} in Eq. (2) over all possible values. The slight gap between the analytical and numerical results is due to a deviation introduced by the first-order approximation $e^{-f(Y_n)} \approx 1 - f(Y_n)$ of Eq. (22) in the proof of Theorem 2. The deviation diminishes as Y_n becomes smaller, so the approximation and the first line of Eq. (20) are more accurate, because Y_n is small near ϕ_{cr} (see Fig. 3.(a) and (b), where Y_n abruptly increases from zero).



(a) Node yield v.s. ϕ_{cr} (b) Type-1 ($\kappa = 0$) (c) Type-2 ($\kappa = 0.8$) (d) Type-2 ($\kappa = 0.2$)

Fig. 5. Illustration of the critical edge disconnection ratio/probability ϕ_{cr} with respect to average physical degree $\bar{k}_p$ in Erdös-Rényi graphs.

Next, we evaluate the analytical ϕ_{cr} in Type-2 scenario (the second line of Eq. (20)), setting $\kappa = 0.8$, and plotting the numerical and analytical ϕ_{cr} versus $\bar{k}_p$ in Fig. 5.(c). We observe a non-trivial gap between the two, which is due to the first and second-order approximations used to obtain Eq. (20). Although the gap is larger than that of Type-1 scenario in Fig. 5.(b), it becomes smaller as the average physical degree $\bar{k}_p$ increases. When κ is decreased to 0.2, as depicted in Fig. 5.(d), the gap is reduced even further. Despite the analytical-numerical gap, Eq. (20) provides a useful indication of ϕ_{cr}'s trend: it increases sub-linearly with $\bar{k}_p$ in Type-2 scenarios, and decreases at least linearly versus κ.

VI. Conclusion

This paper studies the resilience of IoT systems, against edge and jointly-induced cascade-of-failures. The IoT system is modeled as an interdependent network, and the outcome of the cascade is captured by the node yield metric. With the proposed model, we derive node yield as functions of initial disconnecting probability (property of the triggering incident) and node degree distributions (property of network topology). Without knowledge of the exact network topology, node yield can be solved using numerical algorithms for arbitrary degree distributions. Then, a critical initial disconnecting probability is obtained for networks with Poisson degree distributions. Node yield and the critical condition can provide information on the estimated impact of a cascade, the amount of repair needed after the cascade, and required redundancy level in designing a new system. Our work in this paper contributes to the knowledge on network resilience, which will benefit the design, deployment, and operation of real-world IoT systems.

References

[1] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging internet of things marketplace from an industrial perspective: A survey," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, pp. 585–598, Dec 2015.

[2] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, pp. 3–9, Feb 2014.

[3] NIST, "Cyber-physical systems." https://www.nist.gov/el/cyber-physical-systems, 2017. Accessed: 2017-07-28.

[4] O. Yağan *et al.*, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1708–1720, 2012.

[5] Z. Huang *et al.*, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Transactions on Computers*, vol. 64, no. 8, pp. 2158–2168, 2015.

[6] C. Mulliner and J.-P. Seifert, "Rise of the iBots: Owning a telco network," in *MALWARE'10*, pp. 71–80, IEEE, 2010.

[7] A. Arabo, "Cyber security challenges within the connected home ecosystem futures," *Procedia Computer Science*, vol. 61, pp. 227 – 232, 2015. Complex Adaptive Systems San Jose, CA November 2-4, 2015.

[8] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, 2017.

[9] S. V. Buldyrev *et al.*, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[10] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on ieee 802.11ah: An enabling networking technology for smart cities," *Computer Communications*, vol. 58, pp. 53 – 69, 2015. Special Issue on Networking and Communications for Smart Cities.

[11] 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*, vol. 4, no. 1-2, pp. 63–79, 2008.

[12] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Phys. Rev. E*, vol. 83, p. 065101, Jun 2011.

[13] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[14] G. Zhang *et al.*, "Cascading failures of power grids caused by line breakdown," *International Journal of Circuit Theory and Applications*, vol. 43, no. 12, pp. 1807–1814, 2015.

[15] J.-W. Wang and L.-L. Rong, "Edge-based-attack induced cascading failures on scale-free networks," *Physica A: Statistical Mechanics and its Applications*, vol. 388, no. 8, pp. 1731 – 1737, 2009.

[16] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliability Engineering & System Safety*, vol. 145, pp. 47 – 61, 2016.

[17] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures—analysis and control implications," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 2634–2642, IEEE, 2014.

[18] H. Ning, *Unit and Ubiquitous Internet of Things*. CRC Press, 2013.

[19] S. A. Pambudi, W. Wang, and C. Wang, "On the resilience of d2d-based social networking service against random failures," in *Proc. IEEE GLOBECOM 2016*, pp. 1–6, IEEE, 2016.

[20] G. Casella and R. L. Berger, *Statistical inference*, vol. 2. Duxbury Pacific Grove, CA, 2002.

[21] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.

[22] C. Grossmann, H.-G. Roos, and M. Stynes, *Numerical treatment of partial differential equations*, vol. 154. Springer, 2007.

[23] A. Sen *et al.*, "Fault-tolerance in sensor networks," in *Proceedings of IEEE INFOCOM 2006*, 2006.

[24] D. J. Struik, *A source book in mathematics, 1200-1800*. Princeton University Press, 2014.

[25] WolframAlpha, 2016 (accessed July 31, 2016).