Resilience of IoT Systems Against Edge-Induced Cascade-of-Failures: A Networking Perspective

Jie Wang, *Student Member, IEEE*, Sigit Pambudi, *Student Member, IEEE*, Wenye Wang, *Fellow, IEEE*, and Min Song, *Fellow, IEEE*

***Abstract*—Internet of Things (IoT) is a networking paradigm that interconnects physical systems to the cyber world, to provide automation and intelligence via interdependent links between the two domains. Such interdependence renders IoT systems vulnerable to random failures, e.g., broken communication links or crashed cyber instances, because a single incident in one domain can develop into a *cascade-of-failures* across domains, which dissolves the network structure, and has devastating consequences. To answer how robust an IoT system is, this paper studies its *resilience* by examining the impact of edge- and jointly-induced cascades, that is, a sequence of failures caused by randomly broken physical links (and simultaneous failing cyber nodes). Resilience of an IoT system is quantified by two new metrics, the *critical edge disconnecting probability* ϕ_{cr}, i.e., the maximum intensity of random failures the system can withstand, and the cascade length τ_{cf}, i.e., the lifetime of a cascade. For IoT systems with Poisson degree distributions, we derive exact solutions for the critical disconnecting probability ϕ_{cr}, above which an edge-induced cascade will completely fragment the network. We also find that the critical condition ϕ_{cr} marks a dichotomy of the expected cascade length $\mathbb{E}(\tau_{cf})$: for the super-critical ($\phi > \phi_{cr}$) scenario, we obtain $\mathbb{E}(\tau_{cf}) \sim \exp(1-\phi)$ through analysis, while for the subcritical scenario, we observe $\mathbb{E}(\tau_{cf}) \sim \exp(1/1-\phi)$ through simulations. With these results, the final outcome of a cascade can be anticipated upon the initial failures, while the reaction window of time-sensitive countermeasures can be obtained before a cascade fully unfolds.**

***Index Terms*—Interdependent networks, Internet of Things (IoT) architecture, network resilience.**

I. Introduction

INTERNET of Things (IoT) is a networking paradigm that connects numerous physical actuators, i.e., "things," to the cyber world, i.e., the Internet, such that data collected in the physical domain can be timely transferred to applications in the cyber domain, while control commands can be timely distributed to actuators in the physical domain, enabling smart home, factory automation, intelligent transportation, and so on [1]. In the IoT paradigm, sensing and actuation have become a *utility* [2], like electricity and water, that is accessible by *applications*, such as remote medicine and smart appliances. The nature of such a system-of-systems is a networked *application* built upon networked *utility*, i.e., a strongly coupled cyber-physical system (CPS) [3]–[5]. For instance, in a mobile social network (MSN), smartphones (physical nodes) are connected by device-to-device (D2D) communication links in the physical domain, through which the smartphone owners/users (cyber nodes) interact socially in the cyber domain.

As interconnections between the physical and cyber networks strengthen to provide intelligence, such close coupling introduces complex *interdependence* between the two domains, which weakens the IoT system as a network. The reason behind this is the increased susceptibility to *cascade-of-failures*: faults triggered by a single incident in one domain, e.g., a broken communication link or a hacked smart device, can propagate across domains through the interconnecting links, causing a chain of failures [5], [6]. In IoT systems, cascade-of-failures can be especially detrimental due to the following reasons. First and foremost, actuators (physical nodes) in the IoT can directly impact human lives, e.g., a malfunctioning wearable medical device may jeopardize a patient's live. Second, the impact of cascade-of-failures can be further exacerbated by the massive scale of IoT systems [2], [7], e.g., the country-wide blackout in smart grids [8]. Considering the devastating impact of failures, it is crucial to understand how *resilient* IoT systems are, against cascades-of-failures that undermine the underlying topological structure. As key functions of IoT systems rely on both physical and cyber nodes being online, i.e., *connected* to the major component of the network, the crux of the resilience problem is the structural capacity of IoT systems as *interdependent networks*.

A. Related Work

Resilience of a system measures its capability to maintain functions and structure in the face of internal and external changes [9]. Resilience of interdependent networks against random or correlated cascading failures has been addressed from two main aspects: 1) the system's intrinsic capacity to random failures and 2) active cascade-mitigation measures.

The former views resilience as a static characteristic of the interdependent network, which is determined once the

Manuscript received February 15, 2019; revised April 12, 2019; accepted April 15, 2019. Date of publication April 24, 2019; date of current version July 31, 2019. This work was supported in part by the NSF under Grant CNS-1526152 and in part by the Army Research Office (ARO) under Grant W911NF-15-2-0102. *(Corresponding author: Jie Wang.)*

J. Wang and W. Wang are with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606 USA (e-mail: jwang50@ncsu.edu; wwang@ncsu.edu).

S. Pambudi was with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC 27606 USA. He is now with MicroStrategy, Tyson, VA 22182 USA (e-mail: spambudi@ncsu.edu).

M. Song is with the Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ 07030 USA (e-mail: min.song@stevens.edu).

Digital Object Identifier 10.1109/JIOT.2019.2913140

topology is fixed. To this end, impact of a cascade has been examined through the remaining fraction of functional nodes [5], [10], and the amount of control effort to steer the system back to normal operation [11]. On network topology properties, Buldyrev *et al.* [6] founded a critical average node degree below which an interdependent network will eventually collapse. From the perspective of existing IoT systems, what a system operator would care the most is the extreme case, that is, *what is the maximum intensity of initial random failure* the IoT system of interest can withhold?

The latter takes a dynamic view, and studies how to boost resilience at run-time, i.e., upon an on-going cascade. To this end, several algorithms have been proposed for smart grids. For instance, an online deterministic algorithm that selectively sheds load to minimize the total amount of load loss (which translates to number of node crashes in a generic IoT setting) is proposed in [12], while a stochastic algorithm that incorporates noise and model errors based on a sample average approximation method has also been introduced [13]. An interesting observation is that an optimal control scheme with the least amount of load loss must be applied at an intermediate time, which is *halfway* between the onset and the end of the cascade of failures [14]. This prompts an another open question on resilience: *what is the reaction window* against a cascade, for time-sensitive countermeasures?

To study the aforementioned open questions, it is necessary to examine the root cause of a cascade-of-failures in IoT systems. From the perspective of an interdependent network that describes a cyber-physical IoT system, a cascade is triggered by physical/cyber node failures and/or physical/cyber link breakages. Among these, while node-induced cascades, e.g., cascading failures in a smart grid caused by failing generators, have been extensively studied, e.g., [4]–[6] and [10], cascades caused by link breakages have not been addressed. Nevertheless, link (especially physical link) breakage constitutes a major cause of cascades in IoT systems: many IoT applications rely on unstable wireless communication as physical links and consequently suffer from random link breakages, e.g., smart home devices connected by IEEE 802.11ah WiFi-HaLow [7]; wired utility links, such as power lines in smart grids, are underguarded and hence more likely to fail than nodes. Meanwhile, connection to the Internet opens IoT systems to malware [15] and cyber attacks [16], [17], which is especially true for smart home devices that usually do not have strong security measures [16], greatly increasing the probability of cyber node crashes. Therefore, *edge-* and *jointly-induced cascades* in an IoT system are not only much more visible than individual failing nodes but also indicate greater impacts from a networking perspective. While the primary network modeling approach offers comprehensive results on networks with edge-induced cascades in a single network context, e.g., power grids [18] and scale-free networks [19], these results do not extend to the interdependent IoT networks.

B. Our Approach and Contributions

Motivated by the lack of study, this paper addresses the *resilience problem* in IoT systems from a networking perspective, focusing on the more prevalent edge- (and jointly-) induced cascades. Specifically, we aim to answer the following.

1) *Critical Condition:* What is the maximum intensity of random failures that the system can withhold?
2) *Reaction Window:* When will the cascade stop?

These questions are 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. Addressing these challenges, contributions of this paper are summarized as follows.

1) *Modeling:* We develop an analytical framework that captures the complex interdependence across the cyber and physical domains, define a network residual process that numerically describes the time-varying impact of a cascade, and propose new metrics to quantify the resilience of an IoT system from different aspects.
2) *Finding:* Particularly for IoT systems with Poisson degree distribution, we prove the existence of a critical initial edge disconnecting probability ϕ_{cr}, above which the network will fully collapse. For the supercritical ($\phi > \phi_{cr}$) scenario, we find the scaling law of the cascade length $\mathbb{E}(\tau_{cf})$ to be $\exp(1-\phi)$ through analysis, and for the subcritical ($\phi < \phi_{cr}$) scenario, we observe $\mathbb{E}(\tau_{cf}) \sim \exp(1/1-\phi)$ through numerical simulations.
3) *Implication:* We show that our findings on scaling laws and influential factors apply to IoT systems with different topologies, even real-world power grids, which implies the significance of our modeling approach and analysis results to the design of IoT networks.

The rest of this paper is organized as follows. We first introduce the system model and metrics in Section II to formulate the resilience problem in an IoT context. Then in Section III, an analysis framework is established to examine the network residual process under an edge- or jointly-induced cascade, with which the critical initial disconnecting probability ϕ_{cr} is obtained to understand IoT resilience as an innate property of the system. Viewing resilience as a dynamic concept, Section IV studies the cascade length τ_{cf} in both supercritical and subcritical scenarios, to interpret the reaction window at run time. To validate the applicability of the proposed approach and findings, we examine the resilience of a half-synthetic IoT network based on real-world power grids in Section V. Finally, this paper is concluded in Section VI.

II. Resilience Problem of IoT Systems

Capturing its nature as a networked application over networked utility, an IoT system can be modeled as an interdependent network, that is composed of a physical network, a cyber network, and internetwork connections. To formally formulate the *resilience* problem, which refers to the survivability of the interdependent network structure, we introduce the network model, parameterize cascades caused by different triggering incidents, describe the evolving cascade by residual processes, and define resilience metrics in this section.

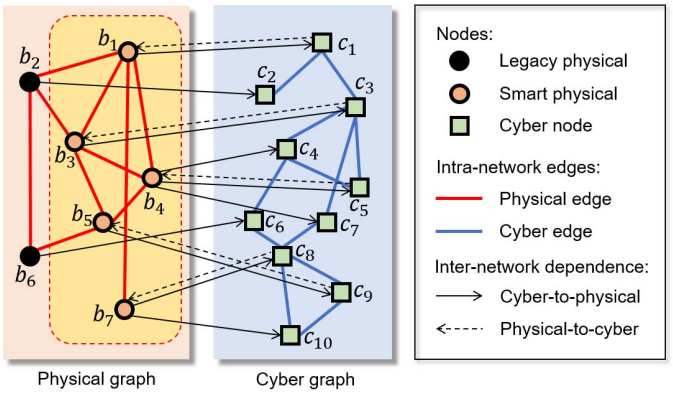


Fig. 1. Interdependent network model $(\mathcal{G}_p, \mathcal{G}_c, \mathcal{E}_{c\to p}, \mathcal{E}_{p\to c})$: internetwork edges capture the support (cyber-to-physical dependence) and control (physical-to-cyber dependence) relationships. For instance, cyber-to-physical edge $e(b_1 \to c_1) \in \mathcal{E}_{c\to p}$ (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 cyber node c_1 *controls* physical node b_1, so b_1 is *dependent* on c_1 as well.

A. Interdependent Network Model of IoT System

We describe the IoT system of interest as an interdependent network[1] $(\mathcal{G}_p, \mathcal{G}_c, \mathcal{E}_{c\to p}, \mathcal{E}_{p\to c})$, illustrated by a simple example in Fig. 1. In this tuple, $\mathcal{G}_p(\mathcal{P}, \mathcal{E}_p)$ denotes the physical network that contains links between physical/utility nodes in set $\mathcal{P} = \{b_1, \ldots, b_{n_p}\}$, while $\mathcal{G}_c(\mathcal{C}, \mathcal{E}_c)$ denotes the cyber network that contains connections between cyber/application nodes 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 the *directed* cross-domain edges in sets $\mathcal{E}_{c\to p}$ and $\mathcal{E}_{p\to c}$. In this model, we assume that one physical node can support multiple cyber nodes (same as [5]), while each physical node is either controlled by one of its supported cyber nodes (smart physical node), or maintaining an isolated control (legacy physical node). To be more specific, for any physical node $b \in \mathcal{P}$:

1) 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 $e(Ct(b) \to b) \in \mathcal{E}_{p\to c}$. We denote $Ct(b) = \varnothing$ if node b is a legacy physical node that maintains an isolated control out of the IoT;
2) there exists a nonempty 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 $\mathbf{B}(n_c, (1/n_p))$;
3) 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 $\alpha = (|\mathcal{P}_s|/|\mathcal{P}|)$ 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 $\mathcal{G}_c$.

B. Triggering Incidents of Cascades

Without loss of generality, denote the time that initial failures (triggering incidents) take place as $t = 0$. As time proceed in discrete slots $\mathcal{T} = \{0, 1, \ldots\}$, initial failures gradually develop into a cascade of failures, due to the consecutive removal of failed nodes/edges. The triggering incidents of cascades can be categorized into three types: 1) node failure; 2) edge disconnection; and 3) joint failures, among which the first two are special cases of the last one. Therefore, we consider a generic triggering incident model, in which each physical edge in $\mathcal{E}_p$ (cyber edge in $\mathcal{E}_c$, respectively) disconnects with probability ϕ_p (ϕ_c), and each physical node in $\mathcal{P}$ (cyber node in $\mathcal{C}$, respectively) fails with probability θ_p (θ_c), where probabilities ϕ_p, ϕ_c, θ_p, and θ_c all take value in $[0, 1]$. In this paper, we choose the following three representative scenarios[2] that are most likely to occur in IoT systems.

1) `Type-0` Scenario: Only physical nodes may crash at time $t = 0$, i.e., $\theta_p > 0$ while $\phi_c = \phi_p = \theta_c = 0$. As the simplest case, it has been studied in [10].

2) `Type-1` Scenario: Only physical links may disconnect at time $t = 0$, i.e., $\phi_p > 0$ while $\theta_p = \theta_c = \phi_c = 0$, corresponding to the most visible initial failures in IoT systems.

3) `Type-2` Scenario: Simultaneous physical link disconnection and cyber node failures take place at $t = 0$, where $\theta_p = \phi_c = 0$ and $\phi_p \geq \theta_c > 0$ because nodes are usually better-guarded than links and are hence less likely to fail.

We combine the latter two cases into a *joint ϕ-edge and $\kappa\phi$-node failure* for the simplicity of notation, where $\phi = \phi_p$ and $\kappa \in [0, 1]$. Particularly, `Type-1` scenario corresponds to the special case of $\kappa = 0$, while $\kappa > 0$ corresponds to `Type-2` scenarios. As a result of such joint initial failures, a set $\mathcal{E}_{\text{fail}}$ of physical links and set $\mathcal{C}_{\text{fail}}$ of cyber nodes are removed from the system at time $t = 0$, with expected values $\mathbb{E}(|\mathcal{E}_{\text{fail}}|) = \phi|\mathcal{E}_p|$ and $\mathbb{E}(|\mathcal{C}_{\text{fail}}|) = \kappa\phi n_c$, respectively.

C. Cascade Process Following Initial Failures

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 time-varying physical network $\mathcal{G}_p(\mathcal{P}_t)$ in the first half of a time slot (odd steps), and the cyber network $\mathcal{G}_c(\mathcal{C}_t)$ in the second half (even steps). Note that $\mathcal{P}_t \subset \mathcal{P}$ and

[1] We introduce the interdependent network model in our prior work [20], and briefly present it here for completeness reasons.

[2] As we will show in our analysis framework, other cases such as cyber link breakage and cyber node fail, can also be analyzed with similar steps after a change of variables, and are hence not presented due to space limit.

$\mathcal{C}_t \subset \mathcal{C}$ are time-decreasing sets of functional nodes at time t. At odd (respectively, even) steps, any physical (cyber) node is deemed as still *functional*, when the following two conditions hold simultaneously: 1) the cyber (physical) node it depends on remains functional, i.e., not removed from the network and 2) itself belongs to the largest connected component (LCC) of the current physical graph $\mathcal{G}_p(\mathcal{P}_t)$ [cyber graph $\mathcal{G}_c(\mathcal{C}_t)$].

In every time step, we examine the two conditions sequentially: physical (cyber) nodes that do not satisfy condition 1) are first singled out, and removed from the current physical graph $\mathcal{G}_p(\mathcal{P}_{t-1})$ [cyber graph $\mathcal{G}_c(\mathcal{C}_{t-1})$], and the resulting network is referred to as the *remaining* physical graph $\mathcal{G}_p(\mathcal{P}'_t)$ [remaining cyber graph $\mathcal{G}_c(\mathcal{C}'_t)$]; then physical (cyber) nodes that fail condition 2) are removed from the remaining graph $\mathcal{G}_p(\mathcal{P}'_t)$ ($\mathcal{G}_c(\mathcal{C}'_t)$), resulting in the *residual* physical network $\mathcal{G}_p(\mathcal{P}_t)$ [residual cyber graph $\mathcal{G}_c(\mathcal{C}_t)$] to be examined again in the following time 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 $\mathcal{E}_{p\to c}$). 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) nodes that remain functional at time t, that is, $R_t^p := (|\mathcal{P}_t|/n_p)$ ($R_t^c := (|\mathcal{C}_t|/n_c)$). 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 nonincreasing in time t. Similarly, we have the remaining node ratios $R_t^{p'} = [(|\mathcal{P}_t{}'|)/n_p]$ ($R_t^{c'} = [(|\mathcal{C}_t{}'|)/n_c]$) as the interim result/process, since $R_{t-1}^p \geq R_t^{p'} \geq R_t^p$ ($R_{t-1}^c \geq R_t^{c'} \geq R_t^c$) for any IoT system under a cascade of failures. As time proceeds, the final *outcome* of a cascade on the interdependent network can be quantified by the *node yield*, which illustrates the worst-case impact of a cascade-of-failures on an IoT system given long enough time, i.e., $Y_n := \lim_{t\to\infty} \mathbb{E}(R_t^p)$.

D. Resilience Metrics

The resilience problem covers two aspects: the 1) *critical condition* of the network under cascades, that is, *to what extend of failure the network can withstand* and the 2) *reaction window*, that is, *when a cascade will stop*, before which countermeasures should be applied. We examine each aspect of the resilience problem with a new resilience metric.

Definition 2 (Critical Disconnecting Probability): Let $Y_n(\phi)$ denote the node yield as a function of the physical edge disconnecting probability ϕ. The critical disconnecting probability ϕ_{cr} is defined as the minimum ϕ that triggers a complete network fragmentation, i.e.,

$$\phi_{cr} := \sup\{0 \leq \phi \leq 1 | Y_n(\phi) > 0\}. \tag{1}$$

Critical condition ϕ_{cr} identifies the maximum intensity of initial failures that the system can survive, which implies at least $\phi_{cr}|\mathcal{E}_p|$ amount of physical edges will need to be removed to fully collapse the network. Apart this "static" resilience metric that is determined at network design stage, we define the cascade length τ_{cf}, to characterize the reaction window of system operators to reflect the system's resilience at run-time.

Definition 3 (Cascade Length): The length of a cascade is defined as the time interval between the onset of a cascade and the stop of the network decomposition, i.e.,

$$\tau_{cf} := \max\left\{ t \geq 0 \middle| \mathbb{E}\left(R_t^{p'}\right) - \mathbb{E}\left(R_{t-1}^{p'}\right) \geq \frac{1}{n_p} \right\} \tag{2}$$

where $R_t^{p'}$ is the ratio of remaining physical nodes at time t.

Intuitively, the cascade length metric describes when the random failure induced cascade stops (when there is almost no change in the remaining node ratio of the physical network), but also identifies the reaction window for countermeasures.

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 $\{P_c(k)\}_k$: upon a cascade induced by a joint ϕ-edge $\kappa\phi$-node failure, is there a critical initial disconnecting probability ϕ_{cr}, above which the network will collapse? What is the expected cascade length $\mathbb{E}(\tau_{cf})$ to apply counter-measures?

III. Resilience as Innate Property: Critical Condition Analysis via Residual Processes

To address the resilience problem, we first follow the evolution of a cascade process in the system, by examining the physical residual process $\{R_t^p\}_t$. Though similar residual processes have been analyzed for node-induced cascades (`Type-0` scenario) in a scale-free interdependent networks of infinite size [5], edge-induced cascades (`Type-1` scenario), and jointly induced cascades (`Type-2` scenario) have not been discussed, despite their prevalence in IoT systems. Therefore, we establish an analysis framework of IoT resilience, as illustrated in Fig. 2, to bridge this gap by mapping `Type-1` and `Type-2` scenarios to equivalent `Type-0` scenarios through an auxiliary graph. Then self-consistent equations of the expected residual physical node ratio $\mathbb{E}(R_t^p)$ are established to theoretically analyze the residual processes in an IoT systems with arbitrary topologies. Finally, we obtain the critical disconnecting probability ϕ_{cr} for IoT networks with Poisson degree distributions.

A. Identifying Key Variables: `Type-0` Scenario

We first identify the key variables to analyze the residual process in the simplest `Type-0` scenario, where a cascade is incurred by physical node failures alone, i.e., physical node are randomly removed with probability θ_p. Consider such a cascade in an interdependent network $(\tilde{\mathcal{G}}_p, \mathcal{G}_c)$, where the physical graph $\tilde{\mathcal{G}}_p(\mathcal{P}, \tilde{\mathcal{E}}_p)$ has degree distribution $\{\tilde{P}_p(k)\}_k$.

After the random node removal in $\tilde{\mathcal{G}}_p$ at $t = 0$, a fraction $(1-\theta_p)$ of the $|\tilde{\mathcal{P}}_p|$ physical nodes remain, so that the remaining ratio $R_t^{p'} = 1 - \theta_p$. The remaining network may further fragment into disconnected components, such that condition 2) of being functional do not hold any more. As a result,

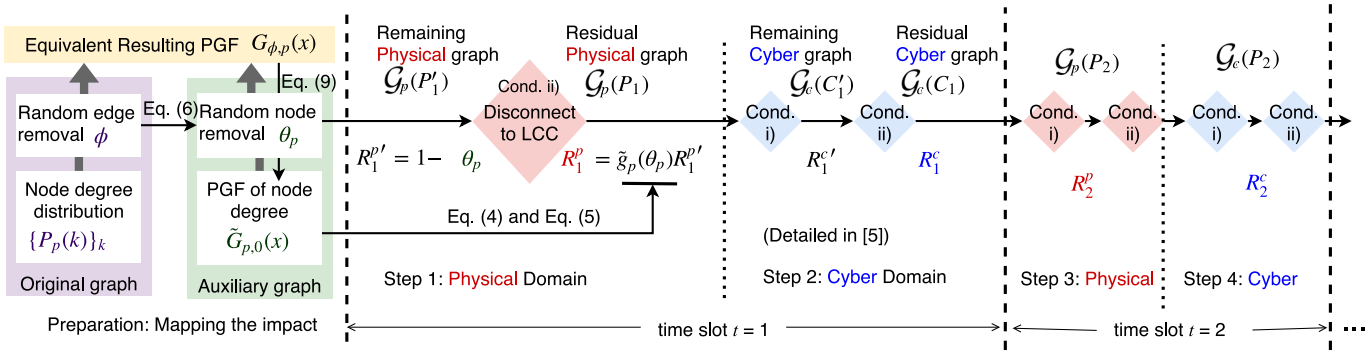


Fig. 2. Architecture of the analysis framework for the resilience problem: first, an auxiliary graph is constructed to convert a Type-1 scenario to an equivalent Type-0 scenario, in the sense that the resulting physical node degree distributions (after initial removal at time $t = 0$) are the same. Then residual processes $\{R_t^p, R_t^c\}_t$ are studied alternatingly for the physical domain and cyber domain, during every time slot, to derive the self-consistent equations stated in Lemma 1.

only a fraction R_t^p of the remaining physical nodes in $\mathcal{P}_t'$ will be the *residual* functioning nodes (set $\mathcal{P}_t$) in the physical graph to be examined in the next step. To obtain this fraction R_t^p, Huang *et al.* proposed a derivation method in [10], which takes advantage of the probability generating function (PGF) $\tilde{G}_{p,0}(x)$ of the degree distribution $\{\tilde{P}_p(k)\}_k$, defined as

$$\tilde{G}_{p,0}(x) := \sum_{k=0}^{\infty} \tilde{P}_p(k) x^k. \tag{3}$$

Let $\tilde{G}'_{p,0}(x) := (d/dx)\tilde{G}_{p,0}(x)$ denote the first-order derivative of $\tilde{G}_{p,0}(x)$, then the fraction of nodes that satisfy condition 2), i.e., $\tilde{g}_p(\theta_p)$ $(= [R_t^p/(R_t^{p'})])$, can be obtained with the help of two supplementary functions, that is,

$$\tilde{g}_p(\theta_p) = 1 - \tilde{G}_{p,1}\big(1 - (1-\theta_p)(1-f_p)\big) \tag{4}$$

where supplementary function $\tilde{G}_{p,1}(x) := \tilde{G}'_{p,0}(x)/\tilde{G}'_{p,0}(1)$ is the derivative normalized by the mean degree (as $\tilde{G}'_{p,0}(1) = \sum_{k=0}^{\infty} k\tilde{P}_p(k)$), and function f_p is the solution to the following transcendental (self-consistent) equation:

$$f_p = \tilde{G}_{p,1}\big(1 - (1-\theta_p)(1-f_p)\big). \tag{5}$$

Note that the residual physical LCC fraction $R_t^p = \tilde{g}_p(\theta_p)$ can then be utilized to derive $R_t^{c\prime}$, R_t^c in the same time slot, and the remaining node ratio $R_{t+1}^{p\prime}$ in the next time slot, as discussed by the step-by-step measure in [5]. Similar results apply to the cyber graph $\tilde{\mathcal{G}}_c$ after random cyber node removal with probability θ_c, and can be obtained by substituting the subscript $()_p$ with $()_c$ and omitting the tilde sign in (4) and (5).

In summary, the key variables to residual process analysis are: the initial node removal probability θ_p, and the PGF $\tilde{G}_{p,0}(x)$ of the node degree distribution $\{\tilde{P}_p(k)\}_k$. Considering that cascades evolve with the same set of node/edge removal rules, despite their different triggering incidents, the open problems of Type-1 and Type-2 scenarios can be solved if we could map the initial *impact* (number of nodes and edges removed) to an equivalent Type-0 scenario by finding out the equivalent θ_p and $\tilde{G}_{p,0}(x)$.

B. From Type-1 and Type-2 to Type-0 Scenarios: Mapping Through Auxiliary Graph $(\tilde{\mathcal{G}}_p, \mathcal{G}_c)$

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 $\{R_t^p\}_t$ of the original network $(\mathcal{G}_p, \mathcal{G}_c)$ under an edge- or jointly-induced cascade, is the same as that of the auxiliary graph $(\tilde{\mathcal{G}}_p, \mathcal{G}_c)$ under a Type-0 cascade, in the sense that the initial impact (removal) at time $t = 0$ are equivalent. We start with the Type-1 scenario, where initial failures are merely random physical edge disconnections, so that both the auxiliary and original cyber graphs remain equal to $\mathcal{G}_c$.

To find the equivalent θ_p and $\tilde{G}_{p,0}(x)$, we deduce the node failure probability θ_p of a Type-0 scenario, and the distribution parameter $\tilde{G}_{p,0}(x)$ of the auxiliary graph [where node failures take place and (4) and (5) hold], from the physical link disconnecting probability ϕ_p of a Type-1 scenario, and the degree distribution parameter $G_{\phi,p}(x)$ of the original interdependent network $(\mathcal{G}_p, \mathcal{G}_c)$.

Right after the random physical edge disconnection, the probability that a physical node $b_i \in \mathcal{P}$ is fully disconnected/isolated, is $\phi^{d_p(b_i)}$. Then from the network's point-of-view, the node removal induced by physical link breakages (Type-1 scenario) is equivalent to that of a Type-0 scenario, where a fraction of θ_p physical nodes are removed at time $t = 0$, so the expected fraction/ratio of physical nodes that are to be removed (due to edge disconnection) is

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

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 (7) against the node degree distribution of auxiliary graph $\tilde{\mathcal{G}}_p$ in Type-0 scenario, 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

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

from [10], 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 θ_p can be obtained from (6). Performing an inversion on (8), finally we have

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

Equations (6) and (9) illustrate how to map the original interdependent network $(\mathcal{G}_p, \mathcal{G}_c)$ under a `Type-1` cascade (parameterized by ϕ, and $\{P_p(k)\}_k$, or equivalently the PGF $\tilde{G}_{p,0}$), to the auxiliary graph $(\tilde{\mathcal{G}}_p, \mathcal{G}_c)$ under a `Type-0` cascade (parameterized by θ_p, and $\{\tilde{P}_p(k)\}_k$, or equivalently the PGF $\tilde{G}_{p,0}(x)$). Note that in this mapping, the set of physical nodes and the cross-domain edges remain the same, while the only difference is the degree distribution in the physical domain.

For a `Type-2` scenario, where random physical edge disconnections are accompanied by 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 section (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.

C. Back to the Original Network: Self-Consistent Equations of the Expected Network Residual Processes

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 residual processes $\{R_t^p\}_t$ and $\{R_t^c\}_t$ (see Definition 1) can be analyzed through self-consistent equations, as shown in the following lemma that holds for IoT systems with arbitrary topologies. This lemma is first presented in our previous work [20], and is included here for later derivation of the cascade length.

Lemma 1 (Expected Physical/Cyber Residual Ratio [20, Lemma 1]): Denote $x_t \coloneqq \mathbb{E}(R_t^p)$ and $y_t \coloneqq \mathbb{E}(R_t^c)$ as the expected residual physical and cyber node ratios of the 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

$$x_t = x_t' \times \tilde{g}_p\big(x_t'\big) \tag{10}$$

and

$$y_t = y_t' \times g_c\big(y_t'\big) \tag{11}$$

where quantities $x_t' \coloneqq \mathbb{E}(R_t^{p\prime})$ and $y_t' \coloneqq \mathbb{E}(R_t^{c\prime})$ are the expected remaining node ratios, and satisfy

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

in which the equivalent node removal probability θ_p can be obtained from (6); remaining LCC fractions $\tilde{g}_p()$ and $g_c()$ can be found in (4).

Proof of Lemma 1 under the `Type-1` scenario follows a similar step-by-step technique in [5, Sec. 5], to which interested readers are directed. For the `Type-2` scenario ($\kappa > 0$) in which physical edges break with probability ϕ and cyber nodes fail with probability $\kappa\phi$, the equivalent impact in the auxiliary graph is the removal of θ_p (which has equivalent impact as the ϕ edge disconnection in the original network) and $\kappa\phi$ fraction of nodes from $\tilde{\mathcal{G}}_p$ and $\mathcal{G}_c$, respectively. Consequently, the fraction of residual nodes (functional in *both* $\tilde{\mathcal{G}}_p$ and $\mathcal{G}_c$) becomes $\theta_p \times \kappa\phi$. In other words, discarding θ_p and $\kappa\phi$ fractions of nodes *separately* is equivalent to removing $(1-\theta_p)(1-\kappa\phi)$ fraction of nodes from *either* graph $\tilde{\mathcal{G}}_p$ or graph $\mathcal{G}_c$ alone. Therefore, we can safely assume that the removal of nodes occur in $\tilde{\mathcal{G}}_p$ alone, to be consistence with `Type-1` scenario ($\kappa = 0$), hence the $(1-\theta_p)(1-\kappa\phi)$ factor in (12). In addition to the inclusion of edge- and jointly-induced cascades, Lemma 1 also caters to the existence of legacy nodes (with the adoption ratio $\alpha < 1$), while results in [5] only hold for the case of $\alpha = 1$. Lemma 1 establishes a time-recursive relationship of the expected residual ratios (x_t, y_t) and the expected remaining ratios (x_t', y_t'), which is the key tool to obtain the desired resilience metrics.

D. Critical Disconnecting Probability ϕ_{cr}

As an innate property of a topological structure, resilience of simple networks is oftentimes quantified by its connectivity [21], which by definition, is the minimum number of edges to be removed before the network becomes disconnected. However, unlike in simple networks where impact of edge removal is immediate, the unfolding impact (cascade-of-failures) of the initial random failures in interdependent networks can only be measured by its *intensity*, i.e., the edge disconnecting probability ϕ (and coefficient κ for `Type-2` scenarios).

Particularly, we examine the critical condition ϕ_{cr} in interdependent networks with Poisson (or binomial if the network size n_p and n_c are finite) degree distributions (Erdös–Rényi or ER graphs), considering that ER graphs have been applied as the underlying network topology in realizing network connectivity and resource distribution for IoT systems [22], e.g., D2D-based MSN at a conference venue [23]. Here, we directly present the result from our previous work [20], in which interested readers can find detailed derivation of ϕ_{cr}.

Theorem 1 (Critical Condition [20, Th. 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

$$\phi_{cr} \approx \begin{cases} 1 - \frac{1.59362}{\bar{k}_p}, & \text{under } \texttt{Type-1} \text{ fault} \\ 1 - \frac{\kappa+1}{\kappa+\bar{k}_p}, & \text{under } \texttt{Type-2} \text{ fault.} \end{cases} \tag{13}$$

Fig. 3(a) shows the validation of Theorem 1 in a `Type-1` scenario (black dashed line), against numerical simulation (red solid line) in an interdependent network ($n_p = n_c = 5000$) with binomial degree distributions ($\bar{k}_p = \bar{k}_c = 10$). The analytical result is obtained by searching for ϕ_{cr} in (1) over all possible values, while the simulation result is obtained by

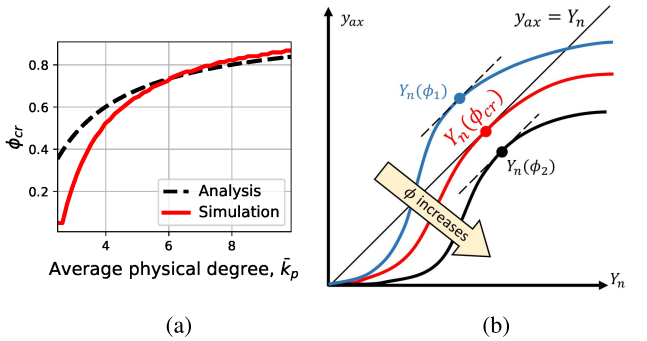


Fig. 3. Critical edge disconnection ratio/probability ϕ_{cr} with respect to average physical degree $\bar{k}_p$ in interdependent network with Poisson degree distributions. (a) `Type-1` ($\kappa = 0$). (b) Node yield versus ϕ_{cr}.

averaging over 5×10^3 realizations. Similar validation for `Type-2` scenarios can be found in [20]. Despite the slight gap between our analysis and numerical simulations, (13) 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. Fig. 3(b) illustrates the physical meaning of the critical disconnecting probability ϕ_{cr}, that is, the largest ϕ to satisfy a nonzero node yield Y_n, obtained by pushing curve $y_{ax} = p_p[1 - \alpha(1 - g_c(p_p g_p(x^*)))]$ [derived by setting $x'_t = x'_{t+1} := x^*$ in the self-consistent equation (12)] to the point that it is tangent with line $y_{ax} = Y_n$.

IV. Resilience at Runtime: Cascade Length

The critical disconnecting probability ϕ_{cr} illustrates the resilience properties of an IoT system from the impact perspective, which also provides guidelines in enhancing the system's resistance to a coming cascade-of-failures as a *prevention* measure in the design stage, e.g., including redundant edges to purposely densify the network. On the other hand, it is sometimes more desirable to apply *control* measures in case of an on-going cascade, which take effect at *run-time* to restore functionality of an IoT system, so that impact to the (vast) users of IoT systems can be alleviated during a cascade. This is especially important to large-scale systems that are deeply integrated into people's daily lives, e.g., the smart grid, because of the devastating consequences of failures. Fortunately, there has been extensive study on accessible run-time countermeasures in such systems, but they require a critical moment, with respect to the lifetime of the cascade, to deploy, in order to unleash the maximum counter-cascade effect, e.g., [14]. Therefore, in this section, we discuss the lifetime of the cascade in such systems, which also functions as the reaction window for system operators.

We are interested in the *expected cascade length*, i.e., $\mathbb{E}[\tau_{cf}]$, where the expectation is taken over an arbitrarily large number of triggering incidents, considering both node failure and edge disconnections occur randomly at $t = 0$. Particularly, we aim to find out how the network structure and initial failures affect the expected cascade length under the supercritical condition ($\phi > \phi_{cr}$), which will lead to a complete network fragmentation, unless countermeasures are applied.

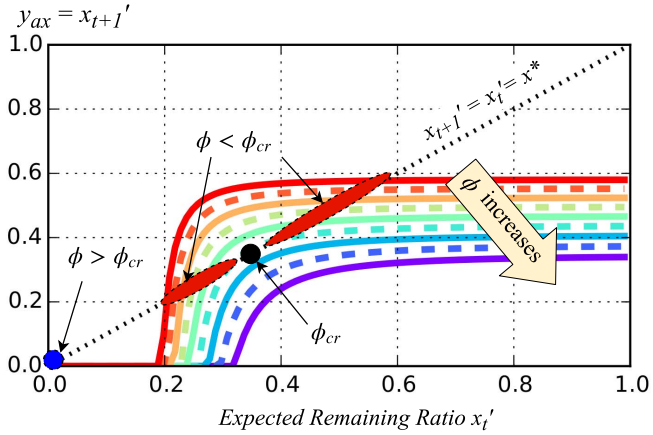


Fig. 4. Determining the stopping point $x'_t = x'_{t+1} = x^*$ of the cascade: solid and dashed curves are the simulation illustration of the self-consistent equations in Lemma 1 as the initial disconnecting probability ϕ increases. (Legends are omitted due to the space limit in the figure.) The red region indicates possible stopping points when $\phi < \phi_{cr}$, while the blue dotted indicates that once ϕ exceeds the critical value ϕ_{cr}, the network will eventually dissolve, and $x^* = 0$ is only possible stopping point in this supercritical scenario.

A. Theoretical Analysis of the Cascade Length

Theorem 2: Consider an IoT system $(\mathcal{G}_p, \mathcal{G}_c)$, whose physical network $\mathcal{G}_p$ has a Poisson degree distribution with mean $\bar{k}_p$, and there are n_c cyber nodes in the cyber network $\mathcal{G}_c$. Upon a `Type-1` physical link breakage with probability $\phi > \phi_{cr}$, the expected cascade length $\mathbb{E}(\tau_{cf})$ scale as

$$\mathbb{E}[\tau_{cf}] \sim \alpha^{-3/2} \exp\left(\frac{\bar{k}_p(1-\phi)}{2(1-\phi_{cr})}\right) \tag{14}$$

where α is the adoption ratio, and ϕ_{cr} is the critical disconnecting probability obtained from Theorem 1.

Proof: Right after the initial physical edges disconnection and cyber nodes failures at time $t = 0$, the expected remaining physical ratio is $x'_{t=0} = 1 - \theta_p$, where θ_p can be obtained with (6). Technically, our analysis starts at time $t = 1$, so to avoid confusion, we denote this ratio as $p_p := x'_{t=0}$ herein.

First, we find the stopping point of the cascade, i.e., the condition that the expected remaining physical node ratio x'_t becomes invariant. Similarly as finding the node yield Y_n and critical condition ϕ_{cr}, we plot curve $y_{ax} = p_p[1 - \alpha(1 - g_c(p_p g_p(x^*)))]$ [derived by setting $x'_t = x'_{t+1} := x^*$ in the self-consistent equations (12) of Lemma 1], against line $y_{ax} = x^*$, as shown in Fig. 4. There are two possible cases: when $\phi < \phi_{cr}$, the final expected remaining node ratio x^* will be strictly larger than 0, and depending on the severeness of initial failure at $t = 0$, which is determined by ϕ, κ, α and degree distributions, the final stopping point could be located in the left or right red region shown in Fig. 4; when $\phi \geq \phi_{cr}$, the only possible stopping point of the cascade is $x^* = 0$, i.e., the IoT network will fully decompose into single nodes, as indicated by the blue dot in the bottom-left corner of Fig. 4. We are interested in the latter case $\phi \geq \phi_{cr}$, which is more hazardous and hence counter-measures are much more needed to stop the IoT system from collapsing.

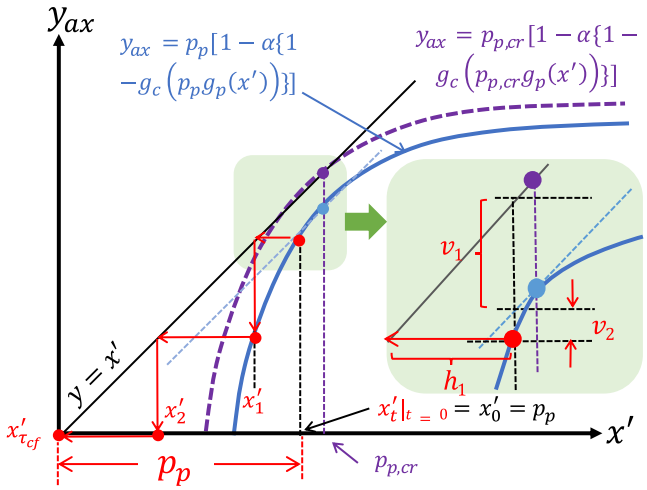


Fig. 5. Illustration of cascade evolution (time t proceeds in $\mathbb{N}^+$) and the cascade length $\mathbb{E}[\tau_{cf}]$ for $\phi > \phi_{cr}$. The vertical distance ($|x'_1 - x'_0|$) of the first step $h_1 = v_1 + v_2$, where distance $v_1 \sim \alpha(p_{p,cr} - x'_0)$ and $v_2 \sim \alpha^2(p_{p,cr} - x'_0)^2$.

Knowing the stopping points of the cascade under different initial failure conditions (parameterized by ϕ), we now obtain the cascade length $\mathbb{E}(\tau_{cf})$, which by definition is the number of time steps t it takes the network fragmentation to stop, i.e., $\min\{t > 0 | x'_{t+1} = x'_t = x^*\}$. Considering the difficulty in deriving a closed-form solution for the self-consistent equations presented in Lemma 1, and to find the subsequent temporal metric τ_{cf}, we derive the cascade length through curve approximation. For the super-critical $\phi > \phi_{cr}$ case, detailed steps to derive $\mathbb{E}(\tau_{cf})$ is shown in Fig. 5.

Let $p_{p,cr}$ denote the initial remaining ratio p_p corresponding to the critical initial edge disconnection ratio ϕ_{cr}. From Lemma 1, we can obtain its value as $p_{p,cr} = 1 - \exp(-\bar{k}_p(1 - \phi_{cr}))$. The cascade length $\mathbb{E}[\tau_{cf}]$ can be restated as: given $x'_0 = p_p < p_{p,cr}$, what is the number of steps until the curve $y_{ax}(x')$ and the solid line $y = x'$ intersects?

To solve this, first note that the vertical distance between the solid blue curve $y_{ax}(x')|_{p_p}$ and dashed purple curve $y_{ax}(x')|_{p_{p,cr}}$, or equivalently, the vertical distance of the blue curve $y_{ax}(x')$ and line $y = x'|_{p_p}$ at $x' = p_{p,cr}$, is proportionate to quantity $(p_p - p_{p,cr})\alpha$, from the curve equations. Then the length of the line segment v_1 in the zoomed subplot of Fig. 5 is also proportionate to quantity $(p_p - p_{p,cr})\alpha$, as the two sets of parallel lines form a parallelogram.

Now if we approximate the (solid blue) curve $y_{ax}(x')|_{p_p}$ with a second-order polynomial,[3] such that the vertical distance v_2 between the shifted (blue dashed) tangent line (with the same slope of 1 as $y = x'$) and the curve $y_{ax}(x')$ can be approximated to be proportional to $\alpha^2(x'_0 - p_{p,cr})^2$. Consequently, both the vertical distance $(v_1 + v_2)$ and horizontal distance $(h_1 = v_1 + v_2)$ between the blue curve $y_{ax}(x')$ and the black line $y = x'$ are proportionate to $\alpha^2(p_{p,cr} - x'_0)^2 + \alpha(p_{p,cr} - x'_0)$, where $x'_0 = p_p$, because line $y = x'$ has a slope of 1. Further, at any point $x' = x'_t$, the horizontal movement speed (distance traversed during one time step) of the red dot is proportionate to $\alpha^2(p_{p,cr} - x'_t)^2 + \alpha(p_{p,cr} - x'_t)$.

Consider a small horizontal distance $\Delta x'$ toward the left of the current point x'_t, the number of steps to traverse distance $\Delta x'$ will be proportionate to $[(\Delta x')/(\alpha^2(p_{p,cr} - x'_t)^2 + \alpha(p_{p,cr} - x'_t))]$. Then, to cover the overall horizontal distance of p_p from the initial remaining ratio x'_0 to the stopping point $x'_{\tau_{cf}}$, as shown in Fig. 5, the total number of steps, i.e., $\mathbb{E}(\tau_{cf})$, is the sum of steps needed for every small distance $\Delta x'$. Therefore, the cascade length can be obtained by an integral, that is,

$$\mathbb{E}(\tau_{cf}) \sim \int_{x'=0}^{p_p} \frac{dx'_0}{\alpha^2\left(x' - p_{p,cr}\right)^2 + \alpha\left(p_{p,cr} - x'\right)} = \pi / \sqrt{\alpha^3\left(p_{p,cr} - p_p\right)} \tag{15}$$

where $p_p = 1 - \theta_p = 1 - \exp(-\bar{k}_p(1 - \phi))$. The integral in (15) can be calculated with results from [24, Sec. 2.103]. Substituting p_p with the initial disconnecting probability ϕ, we have the scaling law as described by (14). ■

Theorem 2 reveals the scaling law of expected cascade length $\mathbb{E}(\tau_{cf})$ in the super-critical scenario, where the initial edge disconnection probability ϕ exceeds the critical value ϕ_{cr}. In this case, the initial failure is severe enough to eventually collapse the network, if no further action is adopted. The scaling law is determined by both the innate network properties (adoption ratio α, mean degree $\bar{k}_p$, and ϕ_{cr}) and severity of the initial failure, captured by ϕ. Specifically, the cascade length scales as $\exp(1-\phi)$ in the super-critical condition under a `Type-1` scenario, where initial failures are due to pure random physical edge disconnections. A direct extension of Theorem 2 gives us the same scaling law in a `Type-2` scenario, because the impact of the cascade in a `Type-2` scenario, i.e., the resulting expected node residuals, are both a constant factor $1-\kappa\phi$ times that under a `Type-1` scenario, as indicated by (12) in Lemma 1. Hence the following corollary.

Corollary 1: Given that $\phi > \phi_{cr}$, the expected cascade length scales as $\mathbb{E}(\tau_{cf}) \sim \exp(1 - \phi)$ for `Type-2` cascades, that is, cascades induced by a joint ϕ-edge $\kappa\phi$-node failure, in IoT networks with Poisson degree distributions.

In addition, from the proof of Theorem 2, i.e., Figs. 4 and 5, we also have the following corollary with respect to the relationship between the two resilience metrics.

Corollary 2: The expected cascade length $\mathbb{E}(\tau_{cf})$ reaches its maximum when the initial disconnecting ratio $\phi = \phi_{cr}$.

The reason behind Corollary 2 is as follows: first, when the initial disconnecting ratio $\phi < \phi_{cr}$, i.e., in the subcritical case, an increase in the number of initially disconnected edges (and failures of cyber node in a `Type-2` scenario) will extend the cascade length τ_{cf}, because in this case, random failures (possible triggers of cascades) take place in broader regions, such that a longer cascade is more likely to be triggered. This trend continues until the longest cascade, the one that nearly fragments the network into isolated nodes, is triggered, i.e., when $\phi = \phi_{cr}$. Beyond this critical point, a severer initial failure will accelerate the cascade process, hence the decrease of the expected cascade length in the super-critical case.

[3]This approximation is reasonable because every function can be represented by a Taylor series (its Taylor's expansion), and in this case we found that the second-order is enough to achieve a small approximation error.

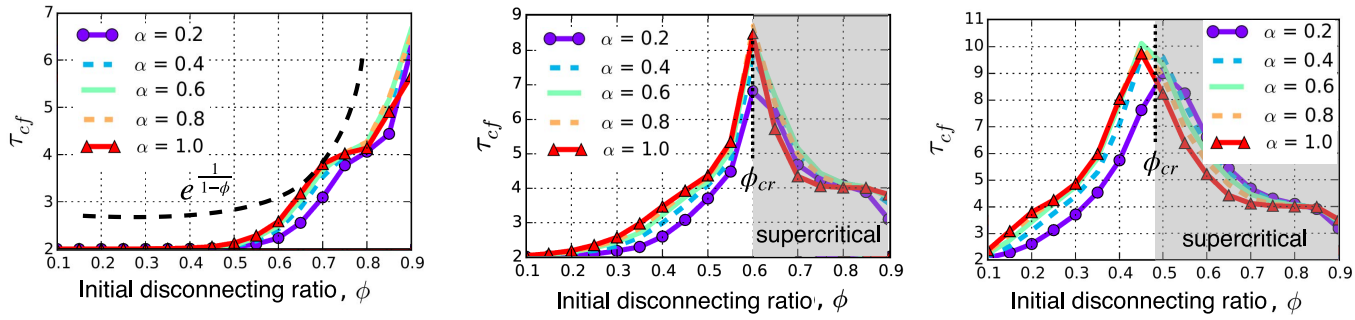


Fig. 6. Expected cascade length $\mathbb{E}[\tau_{cf}]$ (unit: time slots) versus initial disconnecting ratios ϕ for various adoption ratios α. (a) Erdös–Rényi subgraphs, `Type-1`. (b) Erdös–Rényi subgraphs, `Type-2`. (c) Scale-free subgraphs, `Type-2`.

TABLE I
SIMULATION CONFIGURATION

Parameter	Value	Parameter	Value
network realization	10	repetition	100
disconnecting prob. ϕ	$[0.1, 0.9]$	adoption ratio α	$[0.2, 1.0]$
Network with Erdös-Rényi Subgraphs			
network size n_p, n_c	5000	connecting prob.	0.002
degree distribution	Poisson	average degree $\bar{k}_p$,$\bar{k}_c$	10
Network with Scale-free Subgraphs			
network size n_p, n_c	5000	BA [27] model m	3
degree distribution	Power law	average degree $\bar{k}_p$,$\bar{k}_c$	6

B. Numerical Simulation

To verify the theoretic analysis of resilience metrics in the previous Section IV-A, particularly the scaling law of cascade length $\mathbb{E}(\tau_{cf})$ stated in Theorem 2 and Corollary 1, numerical simulations are conducted in interdependent networks with different subgraph topologies, that is, the Erdös–Rényi network (also called random graph) and scale-free network (also called power-law graph). In an Erdös–Rényi network, the node degree distribution is binomial (or approximately Poisson, as network size tends to infinity), which has been used to model IoT systems [22], and D2D-based MSN [23], while in a scale-free network, the node degree distribution satisfies power-law, i.e., $P_p(k) \sim k^{-\beta}$, which has been observed in a lot of real-world networks, including power grids, communication network and Internet [25], [26].

In this section, we assume the physical and cyber subgraphs to be of the same network type (but different topologies/realizations), e.g., both the physical and cyber subgraphs are Erdös–Rényi networks. For each network type, we randomly generate 10 network realizations, for each of which we simulate the cascade propagation process triggered by 100 sets of initial random failures, for every ϕ and α value. Detailed simulation configuration can be found in Table I.

Fig. 6(a) illustrates the cascade length (unit: time slots) over the initial disconnecting probability ϕ in a `Type-1` scenario, which corresponds to the result in Theorem 2.

Since the critical disconnecting probability ϕ_{cr} is large ($\phi_{cr} = 0.875$) in a `Type-1` scenario, it is difficult to examine the supercritical case where $\phi > \phi_{cr}$. However, we observe a quick decreasing cascade length when the disconnecting probability $\phi < \phi_{cr}$ decreases, resembling $\exp(1/1-\phi)$, as shown by the black dashed line in Fig. 6(a).

To better observe the cascade length in a super-critical case, we employ a `Type-2` scenario, whose ϕ_{cr} is lower. Combining Corollary 1 and the observation from Fig. 6(a), we have the following reasonable speculation.

The cascade length of a `Type-2` cascade scales as $\exp(1/1-\phi)$ in the subcritical case, when $\phi < \phi_{cr}$, while as $\exp(1-\phi)$ in the super-critical case, when $\phi > \phi_{cr}$.

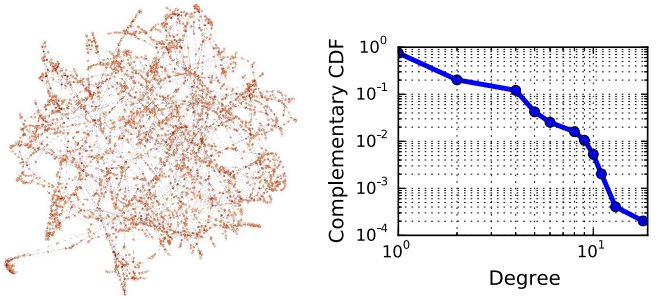
This speculation is confirmed by the numerical simulation results in interdependent networks with both Erdös–Rényi subgraphs [Fig. 6(b)] and scale-free subgraphs [Fig. 6(c)].

C. Observation and Discussion

Further, comparing the cascade length $\mathbb{E}(\tau_{cf})$ and the accompanied critical disconnecting ratio ϕ_{cr} (from Corollary 2) in the two networks, we have the following observations with respect to an IoT system's resilience against failures.

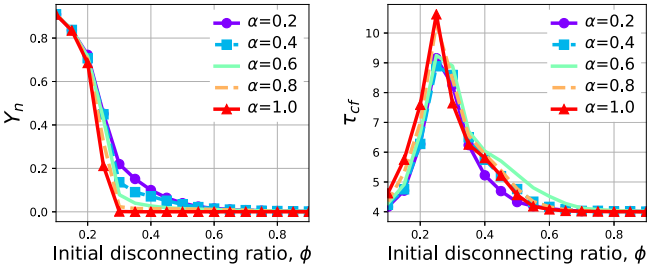
1) Scaling Laws of $\mathbb{E}(\tau_{cf})$ Over ϕ: In both networks, the expected cascade length increases as $\exp(1/1-\phi)$ before ϕ_{cr}, and decreases as $\exp(1-\phi)$ after that.

2) Impact of α on ϕ_{cr}: With respect to the critical initial disconnecting ratio ϕ_{cr}, the impact of adoption ratio α is much more visible in IoT systems with scale-free subgraphs, than that with Erdös–Rényi subgraphs, where there is minimal, if any, impact from α. This phenomenon can be observed by the concentrated (narrow) "peak" in Fig. 6(b), as opposed to the dispersed peaks in Fig. 6(c). The reason behind this is that Erdös–Rényi networks are rather "uniform" in the sense that most nodes in both the physical and cyber subgraph tend to have similar degrees concentrated around the mean degree $\bar{k}_p$ and $\bar{k}_s$. Consequently, initial failures in the cyber graph (in a `Type-2` scenario) are less likely to affect a high-degree physical node, even when the adoption ratio α is high, i.e., when more physical nodes are controlled by cyber nodes. On the contrary, in an IoT system with scale-free (power-law) subgraphs, a high-degree physical node is more likely to be controlled by a low-degree cyber node, as a result of



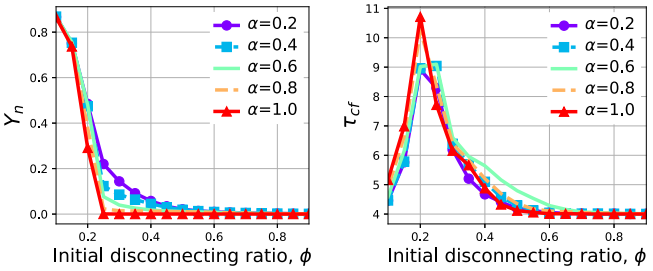
(a) (b)

Fig. 7. Western power grids in U.S. (a) Visualization. (b) CCDF of degree.



(a) (b)

Fig. 8. Resilience of the smart grid in a `Type-1` scenario. (a) Node yield Y_n. (b) Cascade length $\mathbb{E}(\tau_{cf})$.



(a) (b)

Fig. 9. Resilience of the smart grid in a `Type-2` ($\kappa = 0.3$) scenario. (a) Node yield Y_n. (b) Cascade length $\mathbb{E}(\tau_{cf})$.

which, cyber node failures can easily cause more damage in the physical network, especially when α is high.

3) Impact of α on $\mathbb{E}(\tau_{cf})$: In contrast to ϕ_{cr}, the influence of adoption ratio α on the expected cascade length $\mathbb{E}(\tau_{cf})$ is similar in both networks: an increase in α lengthens the cascade process in the subcritical ($\phi < \phi_{cr}$) case, due to the "extra" steps caused by stronger coupling between the physical and cyber networks, while it shortens the cascade process in the super-critical ($\phi > \phi_{cr}$) case, due to the overwhelming failure passed from cyber domain to physical domain. This effect again emphasizes the importance of the critical initial disconnecting ratio ϕ_{cr}, which exists in interdependent networks with both types of subgraphs, and marks the dichotomy in an IoT system's response to cascading failures.

V. Case Study: Resilience of Smart Grid

In this section, we examine the resilience of a real-world IoT system, a smart grid, to further validate the proposed model, metrics, and analysis in networks with complex topologies.

A. Interdependent Network of the IoT System

This half-synthetic smart grid is composed of a real power grid (as physical subgraph $\mathcal{G}_{WS}$) and a synthetic communication network (as cyber subgraph $\mathcal{G}_c$).

1) Physical Subgraph $\mathcal{G}_{WS}$: We consider the power network of the western United States, also known as the western states power grid, which has 4941 nodes and 6594 edges [25], as illustrated in Fig. 7(a). In general, the degree distribution of a power grid $P_p(k) \sim k^{-\beta}$, where the exponent factor β ranges from 2.5 to 4 [26]. This indicates that a typical power grid stands between a scale-free graph ($2 < \beta \leq 3$) and a random (ER) graph ($\beta > 3$), which can be seen from the complementary CDF (CCDF) plot of physical nodes in Fig. 7(b), considering that the CCDF approximates a straight line but with a curved middle-part in the log-log plot.

2) Communication Subgraph $\mathcal{G}_c$: Most communication networks are also observed to have scale-free properties with the exponent β ranging from 2 to 2.6 [26]. To compare with the scale-free networks discussed in Fig. 6(c), we consider the scale-free network with $\beta = 3$ as the communication subgraph $\mathcal{G}_c$, which can be easily generated with the Barabási–Albert model (also known as the preferential attachment model) [27].

B. Resilience Analysis

We simulate cascade processes on the half-synthetic interdependent network $(\mathcal{G}_{WS}, \mathcal{G}_c)$ with the same configuration as shown in Table I, to compare with IoT systems of synthetic network topologies. Numerical results are presented in Figs. 8 and 9, for the `Type-1` and `Type-2` scenarios, respectively. In addition, we employ a finer granularity of initial disconnecting ratio ϕ in $[0.1, 0.4]$ to take a closer look at the expected cascade length $\mathbb{E}(\tau_{cf})$, whose mean (triangle and round markers) and standard deviation (error bars) are shown in Fig. 10.

1) Much Lower ϕ_{cr}: As can be seen from both Figs. 8(b) and 9(b), the critical initial disconnecting ratio ϕ_{cr} of this real world IoT system is much lower than that of the artificial system with scale-free subgraphs shown in Fig. 6(c), due to its low average physical degree $\bar{k}_{WS} = 2.669$. It is no coincidence that the value of ϕ_{cr} at $\alpha = 1$ in $(\mathcal{G}_{WS}, \mathcal{G}_c)$ [ϕ value at the peak of the red line with triangle markers in Fig. 8(b)] is very close to the ϕ_{cr} value at $\bar{k}_p = 2.669$ in Fig. 3(a). Despite the difference in topologies, i.e., degree distributions, the most influential factor to resilience metric ϕ_{cr} is still the mean physical node degree $\bar{k}_p$, especially when $\bar{k}_p$ is low.

2) Same Scaling Laws of $\mathbb{E}(\tau)_{cf}$: The scaling laws of the expected cascade length $\mathbb{E}(\tau)$ over ϕ in $(\mathcal{G}_{WS}, \mathcal{G}_c)$ [all the lines in Fig. 9(b)] remain the same as that in IoT systems with Erdös–Rényi subgraphs [Fig. 6(b)] and scale-free subgraphs [Fig. 6(c)]. The impact of adoption ratio α is also similar, in the sense that ϕ_{cr} marks a dichotomy of its influence on $\mathbb{E}(\tau_{cf})$.

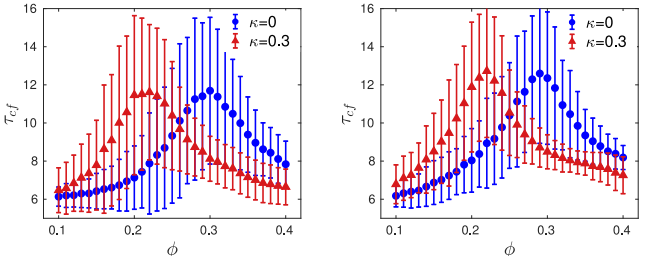


Fig. 10. Cascade length statistics for $\phi \in [0.1, 0.4]$. (a) $\alpha = 0.2$. (b) $\alpha = 0.8$.

3) Impact of κ: As shown in the proof of Lemma 1 and Corollary 1, the coefficient κ has a "shifting" effect on the critical initial disconnecting ratio ϕ_{cr} and the expected cascade length $\mathbb{E}(\tau_{cf})$, which means that increasing κ will result in a shift of the expected cascade length curve along the axis of ϕ. This can be observed by comparing Figs. 8(b) and 9(b). Moreover, both the first-order and second-order statistics are kept for τ_{cf} under this "shift," as illustrated by Fig. 10.

VI. Conclusion

This paper studies the resilience of IoT systems as interdependent networks, against edge- and jointly-induced cascade-of-failures. Viewed as both an intrinsic network attribute that is determined in the design stage, and a dynamic property that can be boosted at run-time, resilience is quantified by the critical disconnecting probability, and the cascade length metrics, respectively. Capturing the network status under a cascade-of-failure process by random processes on the network residuals, we establish self-consistent equations of the expected residuals, from which the critical initial disconnecting probability and cascade length are obtained for IoT networks of different topologies through analysis and simulation. Particularly, our findings also apply to half-synthetic IoT networks based on real-world power grids, indicating the significance of the proposed interdependent network model, characterization of cascades based on initial failure patterns, and the analysis of influential factors. The proposed resilience metrics reveal the structural capacity of an existing IoT system against cascades-of-failures, the required redundancy level in designing a new system, as well as the reaction window of operators to apply run-time countermeasures. Our model, approach, and observations unveil the research direction of run-time resilience-enhancement measures, which are both necessary and prominent in the design of practical 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 Trans. Emerg. Topics Comput.*, vol. 3, no. 4, pp. 585–598, Dec. 2015.

[2] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[3] *Cyber-Physical Systems*, NIST, Gaithersburg, MD, USA, 2017. Accessed: Jul. 28, 2017. [Online]. Available: https://www.nist.gov/el/cyber-physical-systems

[4] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1708–1720, Sep. 2012.

[5] Z. Huang, C. Wang, M. Stojmenovic, and A. Nayak, "Characterization of cascading failures in interdependent cyber-physical systems," *IEEE Trans. Comput.*, vol. 64, no. 8, pp. 2158–2168, Aug. 2015.

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

[7] E. Khorov, A. Lyakhov, A. Krotov, and A. Guschin, "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," *Comput. Commun.*, vol. 58, pp. 53–69, Mar. 2015.

[8] V. Rosato *et al.*, "Modelling interdependent infrastructures using interacting dynamical models," *Int. J. Critical Infrastruct.*, vol. 4, nos. 1–2, pp. 63–79, 2008.

[9] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Rel. Eng. Syst. Safety*, vol. 145, pp. 47–61, Jan. 2016.

[10] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Robustness of interdependent networks under targeted attack," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 83, Jun. 2011, Art. no. 065101.

[11] A. Clark and S. Zonouz, "Cyber-physical resilience: Definition and assessment metric," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1671–1684, Mar. 2019.

[12] D. Bienstock, "Optimal control of cascading power grid failures," in *Proc. 50th IEEE Conf. Decis. Control Eur. Control Conf.*, Dec. 2011, pp. 2166–2173.

[13] J. A. Sefair, J. C. Smith, M. A. Acevedo, and R. J. Fletcher, Jr., "A defender-attacker model and algorithm for maximizing weighted expected hitting time with application to conservation planning," *IISE Trans.*, vol. 49, no. 12, pp. 1112–1128, 2017. doi: 10.1080/24725854.2017.1360533.

[14] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures—Analysis and control implications," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2014, pp. 2634–2642.

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

[16] A. Arabo, "Cyber security challenges within the connected home ecosystem futures," *Procedia Comput. Sci.*, vol. 61, pp. 227–232, Jul. 2015.

[17] 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, p. 87, 2017.

[18] G. Zhang, Z. Li, B. Zhang, D. Qiu, and W. A. Halang, "Cascading failures of power grids caused by line breakdown," *Int. J. Circuit Theory Appl.*, vol. 43, no. 12, pp. 1807–1814, 2015.

[19] J.-W. Wang and L.-L. Rong, "Edge-based-attack induced cascading failures on scale-free networks," *Physica A Stat. Mech. Appl.*, vol. 388, no. 8, pp. 1731–1737, 2009.

[20] S. Pambudi, J. Wang, W. Wang, M. Song, and X. Zhu, "The aftermath of broken links: Resilience of IoT systems from a networking perspective," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–9.

[21] A. Sen, B. H. Shen, L. Zhou, and B. Hao, "Fault-tolerance in sensor networks: A new evaluation metric," in *Proc. IEEE INFOCOM*, 2006, pp. 1–12.

[22] H. Ning, *Unit and Ubiquitous Internet of Things*. Boca Raton, FL, USA: CRC Press, 2013.

[23] S. A. Pambudi, W. Wang, and C. Wang, "On the resilience of D2D-based social networking service against random failures," in *Proc. IEEE GLOBECOM*, Washington, DC, USA, 2016, pp. 1–6.

[24] D. Zwillinger, V. Moll, I. Gradshteyn, and I. Ryzhik, "2. Indefinite integrals of elementary functions," in *Table of Integrals, Series, and Products*, 8th ed. Boston, MA, USA: Academic, 2014, pp. 63–247.

[25] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks," *Nature*, vol. 393, no. 6684, p. 440, 1998.

[26] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 151–159, Mar. 2013.

[27] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

Jie Wang (S'15) received the B.S. and M.S. degrees in electrical engineering from Tongji University, Shanghai, China, in 2010 and 2013, respectively. She is currently pursuing the Ph.D. degree in computer engineering at the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA.

Her current research interests include modeling and analysis of wireless networks, data dissemination, and edge computing.

Sigit Pambudi (S'15) received the B.S. degree in electrical engineering from the Institut Teknologi Bandung, Bandung, Indonesia, in 2009, the M.S. degree in electrical engineering from Yonsei University, Seoul, South Korea, in 2011, and the Ph.D. degree in computer engineering from North Carolina State University, Raleigh, NC, USA, in 2017.

He is currently with MicroStrategy, Tysons, VA, USA.

Wenye Wang (F'17) received the M.S.E.E. and Ph.D. degrees in computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 1999 and 2002, respectively.

She is a Professor with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA. Her current research interests include mobile and secure computing, modeling and analysis of wireless networks, network topology, and architecture design.

Dr. Wang was a recipient of the NSF CAREER Award 2006. She was a co-recipient of the 2006 IEEE GLOBECOM Best Student Paper Award—Communication Networks and the 2004 IEEE Conference on Computer Communications and Networks Best Student Paper Award. She has been a member of the Association for Computing Machinery since 1998 and a member of the Eta Kappa Nu and Gamma Beta Phi honorary societies since 2001.

Min Song (F'18) was the David House Professor, the Chair of the Computer Science Department, and a Professor of electrical and computer engineering with Michigan Technological University, Houghton, MI, USA, from 2014 to 2018. He joined the Stevens Institute of Technology, Hoboken, NJ, USA, in 2018, as a Professor and the Chair of the Department of Electrical and Computer Engineering. His professional career comprises 28 years in academia, government, and industry. He served as the Program Director of the National Science Foundation (NSF) from 2010 to 2014. He was also the Founding Director of the Institute of Computing and Cybersystems, Michigan Technological University. He has authored or coauthored over 165 technical papers and has held various leadership positions.

Prof. Song was a recipient of the NSF CAREER Award in 2007 and the NSF Directors Award in 2012. He served as the TPC Co-Chair for many IEEE conferences, including ICC and GLOBECOM. He has been serving as a member of the IEEE INFOCOM Steering Committee.