How Can Cyber-Physical Interdependence Affect the Mitigation of Cascading Power Failure?

Mingkui Wei*, Zhuo Lu†, Yufei Tang‡ and Xiang Lu§

*Co-Primary Author, Computer Science, Sam Houston State University, Huntsville, TX 77340
†Co-Primary Author, Electrical Engineering, University of South Florida, Tampa, FL 33620
‡Computer and Electrical Engineering, Florida Atlantic University, Boca Raton, FL 33431
§Institute of Information Engineering, Chinese Academy of Science, Beijing, China 100093

***Abstract*—Utilizing advanced communication technologies to facilitate power system monitoring and control, the smart grid is envisioned to be more robust and resilient against cascading failures. Although the integration of communication network does benefit the smart grid in many aspects, such benefits should not overshadow the fact that the interdependence between the communication network and the power infrastructure makes the smart grid more fragile to cascading failures. Thus, it is essential to understand the impact of such cyber-physical integration with interdependence from both positive and negative perspectives. In this paper, we develop a systematic framework to analyze the benefits and drawbacks of the cyber-physical interdependence. We use theoretical analysis and system-level simulations to characterize the impact of such interdependence. We identify two phases during the progress of failure propagation where the integrated communication and interdependence helps and hinders the mitigation of the failure, respectively, which provides practical guidance to smart grid system design and optimization.**

***Index Terms*—Smart grid; failure propagation; cascading failure; load shedding control; modeling and simulations.**

I. Introduction

The modern smart grid [1] is a representative cyber-physical system, in which a layer of communication networking is built upon the conventional power grid to facilitate real-time, intelligent monitoring and control functionalities. Assisted by the communication network, the smart grid is expected to become more resilient and robust against catastrophic events in the power grid, especially cascading failures [2], [3].

In power systems, a cascading failure is a large-scale system outage that originates from a small and sporadic failure in a chaining effect. Particularly, in a power grid, each power transmission line has its capacity to carry power between buses. If the power that flows through a transmission line exceeds its capacity, the line becomes overloaded. An overloaded line will then be disconnected from the system, either proactively by protective devices such as a relay, or passively due to extra heat accumulation and eventual burn down. The disconnection of a transmission line will trigger a power redistribution on the remaining lines in the whole system, which may in turn cause more lines to become overloaded and failed, and eventually forming an unstoppable avalanche in the power grid. The progress of such process is also called failure propagation.

To prevent the failure propagation in the power grid, the most essential step is to eliminate any overload on transmission lines. Load shedding is developed as an effective approach to achieve this objective [4], [5]. The idea of load shedding is straightforward: rather than passively letting the initial failure propagate and cause overloads on more lines, load shedding proactively disconnects a part of loads off the system after the initial failure, such that any overload can be prevented. For load shedding to be effective, it is critical for the power grid to be integrated with a communication network, by which the control center can obtain a global view of the power system and the ongoing failures, thus making the proper decision on the amount and location of load shedding.

Although the communication network indeed facilitates more effective load shedding in the smart grid, it is nonetheless too hasty to conclude that such cyber-physical integration brings no negative impact. In the smart grid, the power infrastructure heavily relies on the communication network for system monitoring and control; at the same time, the network devices depend on the power grid for power supply. Such interdependence can become an undesirable burden and hinder the operation of the power grid in certain circumstances. For instance, a small regional power system outage may cause some networking devices to lose power, and consequently degrade or even paralyze the local communication, which then adversely impedes corresponding reactions in the power grid. An empirical example that the interdependence intensifies failure propagation in the power grid is the 2003 blackout occurred in Italy [6]: the outage of the power grid affected the performance of its control and monitoring network, which in turn disrupted the restoration of the power grid.

Fully understanding the cyber-physical integration with interdependence requires a systematic study of the influence brought from both positive and negative sides. This work is non-trivial since without such guidance, we may find the efforts on smart grid design in vain or towards a biased direction. In the literature, however, we find no such work trying to study the smart grid from this bi-polar perspective. Communication-assisted intelligent load shedding and the failure propagation in interdependent networks have both been studied separately. In particular, existing works either focus on modeling failure propagation and developing optimal load shedding solutions [2], [7], or characterizing the progress of cascading failures in interdependent networks [6], [8]–[10]. To our best knowledge, the work presented in this paper is the first to consolidate the influence of the cyber-physical integration from both perspectives, and systematically study their interaction and impact of failure mitigation.

In this paper, we take a combined analytical and experimental approach to model the interaction and interdependence between the communication network and the power grid, and evaluate the conditions under which such cyber-physical integration is positive or negative. In particular, we develop a micro-view metric $\mathbb{P}(S_k)$, which is the probability that a failure stops propagating after k lines already fail in an interdependent smart grid, to measure the influence that the cyber-physical integration brings to the progress of the failure. Our theoretical analysis identifies two phases of the failure propagation, where the cyber-physical integration incurs opposite effects in the load shedding control process. We then use the IEEE 57-bus, 118-bus and 300-bus systems to validate our theoretical results. Our contributions can be summarized as follows.

- We identify two phases, initial failure accumulation and steady failure propagation, during a cascading failure in the smart grid, where the cyber-physical integration plays opposite roles. Particularly, in the initial failure accumulation phase, the integrated communication is a dominant factor to increase $P(S_k)$, thus helping load shedding to mitigate the failure propagation. However, in the steady failure propagation phase, the interdependence due to the integration of communication networking comes into play and can substantially decrease $P(S_k)$, accordingly degrading the effectiveness of failure mitigation.
- The work in this paper is the first to comprehensively study the influence of the cyber-physical integration in the smart grid. Our work identifies that the integration brings both positive and negative impacts to the mitigation of failure propagation by load shedding. We further use simulations with standard IEEE power system configurations to present its validity. Our work is meaningful in that it bridges two tightly-coupled research areas, whose correlation has not yet been systematically explored.

The rest of this paper is organized as follows. In Section II, we introduce the system models and state our research problems. In Section III, we demonstrate our theoretical analysis and conclusion in addressing the research problem. In Section IV we use system-level simulations to validate our theoretical analysis. In Section V, we present related work, and in Section VI we conclude this paper.

II. Background, Models and Problem Statement

In this section, we present the smart grid system model, define the cyber-physical interdependence and the failure propagation process. Then, we define two load shedding control policies, and finally state our research problems.

A. Cyber-Physical System and Interdependence Modeling

The smart grid [1] represents the next-generation power system with a layer of communication networking built upon power infrastructures to facilitate real-time, intelligent monitoring and control functionalities. In this paper, we define a smart grid as a cyber-physical system with cyber and physical domains in the following.

Definition 1 (Cyber-Physical Power System Modeling): A smart grid is a cyber-physical power system denoted by a graph pair $\mathcal{G} = \{\mathcal{G}_p, \mathcal{G}_c\}$, where

- $(\mathcal{G}_p = \mathcal{V}_p, \mathcal{E}_p)$ is the graph for the physical domain with $\mathcal{V}_p$ being the set of physical nodes and $\mathcal{E}_p$ being the set of physical links. Any link $e \in \mathcal{E}_p$ can be written as $e = (u, v)$ denoting that it connects nodes u and v $(u \neq v)$ with $u, v \in \mathcal{V}_p$. There exists a power generator, denoted by node $g^* \in \mathcal{V}_p$.
- $\mathcal{G}_c = (\mathcal{V}_c, \mathcal{E}_c)$ is the graph for the cyber domain with $\mathcal{V}_c$ being the set of cyber nodes and $\mathcal{E}_c$ being the set of cyber links. Any link $e \in \mathcal{E}_c$ can also be written as $e = (u, v)$ denoting that it connects nodes u and v $(u \neq v)$ with $u, v \in \mathcal{V}_c$. There exists a control center, denoted by node $c^* \in \mathcal{V}_c$.

In Definition 1, the physical domain $\mathcal{G}_p$ and the cyber domain $\mathcal{G}_c$ are not independent because communication-enabled control plays an essential role in the smart grid. In the following, we define the interdependence models.

Definition 2 (Dependence of Physical Nodes on Cyber Nodes): When a cyber node $u \in \mathcal{G}_c$ serves as the communication interface to a physical node $v \in \mathcal{G}_p$ for any control or monitoring purpose, we say the physical node v *depends on* the cyber node u.

Definition 3 (Dependence of Cyber Nodes on Physical Nodes): When a physical node $v \in \mathcal{G}_p$ supplies power to a cyber node $u \in \mathcal{G}_c$, we say the cyber node u *depends on* the physical node v.

Definition 4 (The 1-β Interdependence): In the 1-β interdependence model, each physical node depends only on one cyber node; and each physical node provides power to $\beta \geq 0$ cyber nodes that depends on it. The power generator $g^* \in \mathcal{V}_p$ does not depend on any cyber node and the control center $c^* \in \mathcal{V}_c$ does not depend on any physical node either.

Remark 1: In Definition 4, a physical node must have exactly one cyber node to serve as the communication interface for the monitoring and control purpose. More communication nodes are unnecessary to serve the same purpose. In contrast, a physical node can supply power to multiple cyber nodes as the cyber domain may have additional devices, such as routers and switches, which serve only for networking functionality. Moreover, β is allowed to be zero. This does not imply that cyber nodes are able to work without power, but means that cyber nodes, such as the control center, have auxiliary power supplies (or simply batteries in many cases) when the main power supply from the physical domain is no longer available. In practice, backup power supplies are indeed widely deployed in power systems [11], [12]. That is, $\beta = 0$ indicates the non-interdependence case in which the cyber domain always functions regardless of power failures in the physical domain.

Fig. 1 shows an example of one-one interdependence ($\beta = 1$) between the cyber and physical domains: a link is drawn from cyber node a to physical node A because node A supplies power to node a (or node a depends on node A); at the same

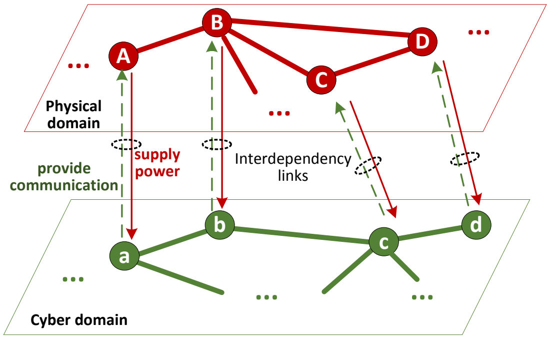


Fig. 1: Modeling of cyber-physical power system.

time, another link is drawn from physical node A to cyber node a because node a provide communication to node A (or node A also depends on node a).

B. Modeling of Failures

We aim to investigate how interdependence affects the failure mitigation in the cyber-physical power system $\mathcal{G}$. It is essential to understand how failures happen and define the failure models for both cyber and physical nodes. In power engineering, a physical node denotes a power infrastructure or a power substation [9]. The failure of such a node is rarely the initial cause of failure propagation, unless there is an intentional damage (e.g., terrorist attack). More often, the failure of a power line between two physical nodes is the initial cause, such as in the Northeast blackout of 2003 [13].

When the initial power line fails (i.e., when the triggering failure happens) due to an accidental short circuit, overheat, or natural disasters [13], it is immediately removed from the physical domain. Then, the power flow in the physical domain has to be redistributed according to Kirchhoff Laws, and all the remaining power lines in the physical domain may experience load changes. A power load increase greater than the capacity of a power line can make the power line overloaded and eventually fail (if there is no failure mitigation) [14]. Accordingly, the power redistributions and failures continue. With more and more power lines failing, a physical node may have no path to the power generator. Once all physical nodes that a cyber node depends on have no path to the generator, the cyber node will not function as it loses its power supply (unless $\beta = 0$). We formally define such a failure process as follows.

Definition 5 (Failure Process of the Cyber-Physical System): Denote the cyber-physical power system after k power line failures by $\mathcal{G}(k) = \{\mathcal{G}_p(k), \mathcal{G}_c(k)\}$, where $\mathcal{G}_p(k) = \{\mathcal{V}_p, \mathcal{E}_p(k)\}$ and $\mathcal{G}_c(k) = \{\mathcal{V}_c, \mathcal{E}_c(k)\}$. When the $(k+1)$-th power line fails, we remove it from $\mathcal{E}_p(k)$ and write

$$\mathcal{E}_p(k+1) = \mathcal{E}_p(k) - \{\text{the } (k+1)\text{-th failed line}\}. \quad (1)$$

When the removing in (1) leads to a cyber node losing its power supply according to the interdependence model in Definition 4, we further remove all its associated cyber edges from the $\mathcal{E}_c(k)$ and write

$$\mathcal{E}_c(k+1) = \mathcal{E}_c(k) - \{\text{all edges of nonfunctional cyber nodes due to the } (k+1)\text{-th failure}\}. \quad (2)$$

It holds for the initial system that $\mathcal{G}(0) = \mathcal{G}$.

C. Load Shedding Control Policies

Communication-enabled control has been widely considered as one of the prominent features in the smart grid. To stop failure propagation, load shedding [9], [14]–[16] as a power control mechanism, has been well investigated in the literature. In load shedding, a cyber node that detects the failure of a power line sends the information to the control center, node $c^* \in \mathcal{V}_c$. Then, upon receiving such information, the control center computes which load in the physical domain should be shed such that (i) the power flow can be re-balanced in the power system without any power line overload and (ii) the load shedding cost is minimized (usually the cost is measured by the total amount of loads to shed). Finally, the control center sends the load shedding command to the cyber node that controls the physical node to shed the load with the computed amount. Each detected power line failure will trigger a load shedding control action in the system.

When the cyber domain does not depend on the physical domain (i.e., when $\beta = 0$), load shedding information can be sent to anywhere in the cyber domain. When $\beta \geq 1$, given the failure process model in Definition 5, cyber nodes may not function due to loss of power. It is likely that a "blind" control center can first compute the optimal load to shed, and then send the command to the cyber node that already loses its power in the cyber domain. Recent load shedding control work [9] considered this interdependence scenario and slightly changed the control policy, in which the control center, aware of the interdependence and the failure progress, must choose to shed the loads from physical nodes with communication interfaces to cyber nodes that are still working. We define the two load shedding control policies in the following.

Definition 6 (Load Shedding Control): When the cyber-physical system $\mathcal{G}$ has k power lines already failed, the control center can make its load shedding decision (i) based on the initial graph pair $\mathcal{G}(0) = \{\mathcal{G}_p(0), \mathcal{G}_c(0)\}$, called *blind load shedding control*, or (ii) based on $\mathcal{G}(k) = \{\mathcal{G}_p(k), \mathcal{G}_c(k)\}$ defined in Definition 5, called *interdependence-aware load shedding control*.

Blind control works based only on the initially deployed system; while interdependence-aware control performs based on the current system excluding cyber nodes that already lose power. It is apparent that interdependence-aware control should outperform blind control in an interdependent cyber-physical system. We aim to quantitatively measure its advantage over the blind one.

D. Problem Statement

It is vital to define a performance metric to characterize the failure process in interdependent systems under load shedding control. A lot of works [5], [14], [17] use the total number of failed power lines. Such a macro-view metric captures the final snapshot of the failure and can be easily measured in simulations. However, existing studies [9], [15], [18] have shown the difficulty to use the metric to understand the evolving characteristics during the failure process in an analytical way.

In this paper, we look at the problem from the micro perspective. We aim to understand how failures happen step by step. In particular, we consider the triggering power line failure as the first failure and denote by S_k the event that the k-th load shedding control prevents the $(k+1)$-th failure from happening given k power lines already failed. As Fig. 2 shows, event S_1 means that the first control stops the second failure given the triggering failure already happening; S_1^c means that give the first failure, the control does not stop the second failure, which makes the failure process continue. When the second failure happens, the second control will be performed with intent to stop the failure again. The failure will stop if S_2 happens, and continue otherwise. As a result, $\{S_k\}_{k\geq 1}$ captures step-by-step details during failure propagation.

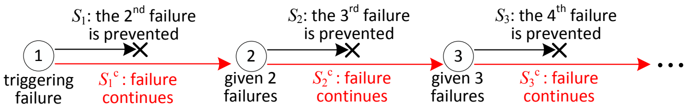

S_1: the 2nd failure is prevented
S_2: the 3rd failure is prevented
S_3: the 4th failure is prevented
1
triggering failure
S_1^c: failure continues
2
given 2 failures
S_2^c: failure continues
3
given 3 failures
S_3^c: failure continues
...

Fig. 2: Example of the failure propagation process with S_1, S_2, and S_3.

We aim to investigate the property of $\mathbb{P}(S_k)$ when k starts from 1. In this way, we can understand the impacts of interdependence and control policies during failure propagation. Given all defined models in the cyber-physical system $\mathcal{G}$, we address two major research questions.

- How to analyze $\mathbb{P}(S_k)$ under different load shedding control and interdependence models?
- What is the cost to improve $\mathbb{P}(S_k)$ under an interdependent cyber-physical system model?

We use both theoretical modeling and standard IEEE power system simulations to answer these questions.

III. Impact of Cyber-Physical Dependence Model on the Performance of Load Shedding

In this section, we first develop the theoretical approach to analyze $\mathbb{P}(S_k)$. Then, we state and discuss our main results. Finally, we prove the main results.

Notations: We write $f(x) = O(g(x))$ or $g(x) = \Omega(f(x))$ if $\exists\, x_0 > 0$ and constant c_0 such that $f(x) \leq c_0 g(x)\ \forall x \geq x_0$. We write $f(x) = \Theta(g(x))$ if $f(x) = O(g(x))$ and $f(x) = \Omega(g(x))$. We write $f(x) = o(g(x))$ if $\forall \epsilon > 0$, $\exists\, x_0 > 0$ such that $f(x) \leq \epsilon g(x)\ \forall x \geq x_0$. We use $o(1)$ to denote a function converging to 0. Given a set $\mathcal{A}$, $|\mathcal{A}|$ denotes the number of elements in $\mathcal{A}$.

A. Theoretical Approach and Main Results

Power failure propagation is a complicated process [9], [15], [18]. Existing studies use simplified power network models [5] or simulations [14] to analyze the process of failure propagation. However, in the scope of this paper, interdependence, random communication network property, and different control policies make the process even more complex. Realizing that power systems and communication network have been modeled as random graphs in the power [19] and network [20]–[22] research communities, respectively, our approach is to model the failure process as the devolution of two random graphs [23] coupled according to Definition 5.

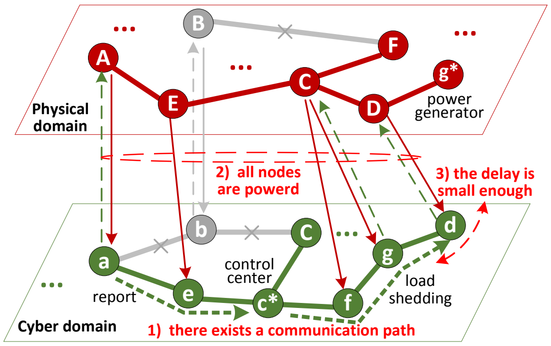


Fig. 3: Conditions for the event S_k happening.

Definition 7 (Random Graph Devolution): A random graph is denoted as $\mathcal{R}(n,p)$, where n is the number of nodes and p denotes the connectedness probability, i.e., the probability that two nodes are connected by an edge. Let the cyber-physical failure process in Definition 5 yield two devolving random graphs satisfying $\mathcal{G}_p(k) = \mathcal{R}(n, p(n,k))$ and $\mathcal{G}_c(k) = \mathcal{R}(m, q(m,k))$, where $n = |\mathcal{V}_p|$, $m = |\mathcal{V}_c|$, and $p(n,k)$ and $q(m,k)$ are connectedness probabilities for the physical and cyber domains, respectively.

In practice, the cyber and physical domains should always be connected when initially deployed. Therefore, we let the initial random graphs $\mathcal{R}(n, p(n,0))$ and $\mathcal{R}(m, q(m,0))$ satisfy

$$p(n{,}0) = \Theta\left(\frac{\log n}{n}\right) > \frac{\log n}{n} \text{ and } q(m{,}0) = \Theta\left(\frac{\log n}{n}\right) > \frac{\log m}{m} \tag{3}$$

to make sure that they are connected asymptotically almost surely (a.a.s.) because of the random graph property [23].

Given the random graph devolution model in Definition 7, our approach is to characterize $\mathbb{P}(S_k)$. The event S_k happening means that the cyber-physical system has already devolved from $\mathcal{G}(0)$ to $\mathcal{G}(k)$, based on which the load shedding is successfully finished before the $(k+1)$-th power line fails. This indicates that the following three events must happen at the same time, as shown in Fig. 3.

1) There must exist a communication path in the cyber domain, which includes the cyber node that reports the failure event, the control center, and the cyber node that receives the load shedding command.
2) All the cyber nodes on the communication path must have power supply; i.e., each of them must depend on at least one physical node in the physical domain that has a physical path to the power generator.

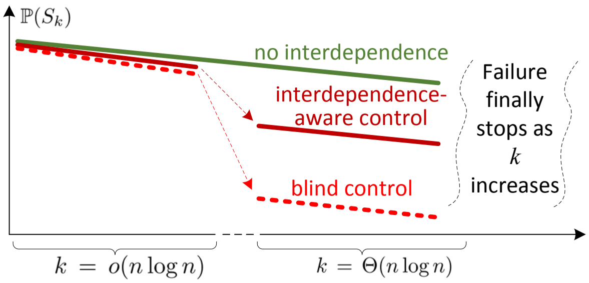


Fig. 4: Illustrative example to characterize $\mathbb{P}(S_k)$.

3) The overall end-to-end delay on the communication path in the cyber domain be must smaller than the time interval from the k-th failure to the next $(k+1)$-th one.

Based on these three events and the random graph devolution model, we analyze $P(S_k)$ by considering two cases: (i) $k = o(n \log n)$, which represents the scenario in which the cyber-physical power system $\mathcal{G}$ just starts to fail and k is small. We call it initial failure accumulation. (ii) $k = \Theta(n \log n)$, reflecting the scenario that a substantial number of power lines have already failed throughout the system, which is called steady failure propagation. We present and discuss our main results in the two cases as follows. We will prove these results in Section III-B.

1) Initial Failure Accumulation:

Theorem 1: When $k = o(n \log n)$, it holds that

$$\mathbb{P}(S_k) = (1 - o(1))\mathbb{P}(d_k < D_k). \tag{4}$$

regardless of the interdependent model and the load shedding control policy, where D_k is the time interval between the k-th and $(k+1)$-th failures, and d_k is the random communication delay between the instant that the source cyber node sends out the power line failure report and the instant that the destination cyber node receives the load shedding commands and acts on the physical domain.

Fig. 4 shows an illustrative example to help understand how $\mathbb{P}(S_k)$ can be characterized during the failure process according to Theorem 1. It can be observed from the $k = o(n \log n)$ part of Fig. 4 that $\mathbb{P}(S_k)$ has approximately the same value (i.e., $\mathbb{P}(S_k) \approx \mathbb{P}(d_k < D_k)$) regardless the interdependence model or control policy.

2) Steady Failure Propagation:

Theorem 2: When $k = \Theta(n \log n)$, it satisfies that

$$\mathbb{P}(S_k) = \begin{cases} (1 - o(1))\mathbb{P}(d_k < D_k) & \beta = 0 \\ \eta\theta(1 - o(1))\mathbb{P}(d_k < D_k) & \beta > 0, \end{cases} \tag{5}$$

where the positive constants $\eta < 1$ and θ satisfies

$$\begin{cases} \theta = 1 & \text{interdependence-aware control} \\ \theta < 1 & \text{blind control.} \end{cases} \tag{6}$$

Observing the $k = \Theta(n \log n)$ part of Fig. 4, we can find that $\mathbb{P}(S_k)$ drops to a smaller value under the interdependence model. More specifically, interdependent-aware load shedding performs better than blind load shedding (by a factor of $\theta < 1$ as indicated in Theorem 2). Note that as shown in Fig. 4, when k keeps increasing and is sufficiently large, the failure propagation will eventually stop because the system has become fully disconnected.

Remark 2: Our results in fact reveal both positive and negative sides of cyber-physical integration: on one hand, during initial failure accumulation, the performance of the integrated communication network is a dominant factor for helping load shedding control to mitigate the failure propagation; on the other hand, during steady failure propagation, the interdependence in such integration comes into play and can substantially degrade the effectiveness of failure mitigation.

3) Improving Control Effectiveness and Associated Cost: Our characterizations of $\mathbb{P}(S_k)$ in initial failure accumulation and steady failure propagation offer insights into the design and optimization of communication-enabled control in an interdependent cyber-physical power system.

- Theorem 1 and Fig. 4 show that the effectiveness of load shedding control during initial failure accumulation is dominated by $\mathbb{P}(d_k < D_k)$. Such a probability is in fact difficult to obtain analytically [15], but it depends on the communication delay performance and the power flow capacity of power lines (i.e., more capacity indicating that a power line can last longer when overloaded [18]). Hence, improving the power line capacity in the physical domain or improve the communication bandwidth in the cyber domain is the most important factor to stop failure propagation during initial failure accumulation. According to (3), there are at least $\Theta(n \log n)$ power and communication lines for the initial deployment of the cyber-physical system $\mathcal{G}$ given n physical nodes, the associated cost to improve the capability of each power line or the bandwidth of each communication line is at least $\Theta(n \log n)$.
- Theorem 2 and Fig. 4 show that interdependence and control policies come into play during steady failure propagation. Interdependence-aware control must be used to improve the control effectiveness. This only incurs a slight additional amount of computational cost [9]. In addition, we can also cut the interdependence between the cyber and physical domain by providing additional power supplies (e.g., battery systems) to communication devices. This will substantially improve the control effectiveness. The associated cost is βn as there are $m = \beta n$ communication devices under the 1-β interdependence model. We can see that cutting interdependence results in a cost of lower order than the $\Theta(n \log n)$ cost in improving communication bandwidth or power line capacity, but it does not substantially help the control effectiveness during the initial failure accumulation.
- Summarizing both Theorem 1 and Theorem 2 in connection to reality, we can conclude that during the initial failure accumulation phase, the integration of communication brings more benefits to the control of the power grid and the failure mitigation. However, as the failure progresses, the number of failed lines in the power grid increases, which results in more communication nodes to be out of service. When the

TABLE I: The methods to improve control effectiveness.

Method	Substantially improve control effectiveness in		Cost
	Initial failure accumulation?	Steady failure propagation?	
Increase power line capacity	Yes	Yes	$\Theta(n\log(n))$
Increase commun. bandwidth	Yes	Yes	$\Theta(n\log(n))$
Cutting interdependence	No	Yes	$\Theta(n)$
Interdepen.-aware control	No	Yes	Extra computations

failure propagation leaves the initial failure accumulation phase and enters the steady failure propagation phase, we observe that the cyber-physical interdependence begins to hinder the failure mitigation process. As shown in Fig. 4, even the interdependence-aware control still under-performs the non-interdependence case. This observation calls for a more reliable design in the cyber domain. For instance, sufficient backup power should be in place to prevent the phase transition from initial failure accumulation to the steady failure propagation.

Table I summarizes all potential methods to improve the control effectiveness with associated costs.

B. Proofs of Main Results

Proof of Theorem 1: The event S_k happening means that the three aforementioned events happen at the same time (as the example shown in Fig. 3). According to the failure process modeling in Definition 5, the first two events, namely, 1) existence of a communication path and 2) all nodes on the path being powered, are equivalent to the event that there exists a path in the cyber domain $\mathcal{G}_c(k)$. Denote by D_k the time interval starting from the instant that the k-th failure happens to the instant that the $(k+1)$-th failure happens. Denote by d_k the communication delay from the instant that the source cyber node reports the failure information to the instant that the destination cyber node receives the load shedding command. We have

$$\mathbb{P}(S_k) = \mathbb{P}(\text{path exists in } \mathcal{G}_c(k))\mathbb{P}(d_k < D_k). \tag{7}$$

To analyze $\mathbb{P}(\text{path exists in } \mathcal{G}_c(k))$, we notice that according to Definitions 5 and 7, $\mathcal{G}_c(k)$ is the k-th devolved version from the random graph $\mathcal{G}_c(0)$ by cutting edges of non-powered cyber nodes, which is determined by the physical domain $\mathcal{G}_p(k) = \mathcal{R}(n, p(n,k))$. After k lines fail in the physical domain, based on (3), we have

$$p(n,k) = p(n,0) - \frac{2k}{n(n-1)} \tag{8}$$

The largest component (i.e., the largest connected subgraph) in the random graph $\mathcal{G}_p(k)$ has $G_p(n,k)$ physical nodes satisfying a.a.s.,

$$G_p(n,k) = \begin{cases} an & p(n,k)n = c_p > 1 > a > 0 \\ n & p(n,k)n > \log n. \end{cases}$$

When $k = o(n\log n)$, we obtain from (8) that

$$p(n,k) = p(n,0) - \frac{2o(n\log n)}{n(n-1)} = p(n,0) - o\left(\frac{\log n}{n}\right), \tag{9}$$

It follows from (3) and (9) that $p(n,k) > \frac{\log n}{n}$ asymptotically. Then, a.a.s., $G_p(n,k) = n$. Given the 1-β interdependence in Definition 4, when $\beta = 0$, $\mathbb{P}(\text{path exists in } \mathcal{G}_c(k)) = 1$ because the cyber domain is independent and connected; when $\beta \geq 1$, $G_p(n,k) = n$ indicates that all physical nodes are connected, and accordingly $m = \beta n$ cyber nodes are all powered a.a.s., which results in $\mathbb{P}(\text{path exists in } \mathcal{G}_c(k)) = 1 - o(1)$. Therefore, we obtain

$$\begin{aligned} \mathbb{P}(S_k) &= \mathbb{P}(\text{path exists in } \mathcal{G}_c(k))\mathbb{P}(d_k < D_k) \\ &= (1 - o(1))\mathbb{P}(d_k < D_k), \end{aligned}$$

which finishes the proof. □

Proof of Theorem 2: When $k = \Theta(n\log n)$, it follows from (8) that

$$p(n,k) = p(n,0) - \frac{\Theta(n\log n)}{n(n-1)} = p(n,0) - \Theta\left(\frac{\log n}{n}\right), \tag{10}$$

if $p(n,0) = \Theta\left(\frac{\log n}{n}\right)$, then $G_p(n,k)$ will first become an during the random graph devolution process with other components only having $O(\log n)$ nodes in the physical domain, as illustrated in Fig. 5.

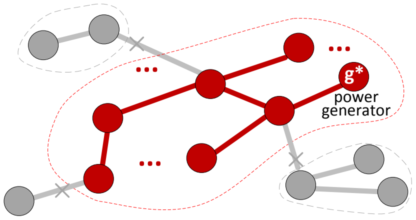


Fig. 5: Components from random graph devolution.

The power generator g^* exists in the $G_p(n,k)$ component with probability $a(1-o(1))$; i.e.,

$$\mathbb{P}(g^* \text{ in } G_p(n,k)) = a(1 - o(1)). \tag{11}$$

In any other $O(\log n)$ component with probability $1 - a(1 - o(1))$. Let event $E_k = \{\text{path exists in } \mathcal{G}_c(k)\}$ Then,

$$\begin{aligned} \mathbb{P}(E_k) = \mathbb{P}(E_k | g^* \text{ in } G_p(n,k))\mathbb{P}(g^* \text{ in } G_p(n,k)) + \\ \mathbb{P}(E_k | g^* \text{ in others})\mathbb{P}(g^* \text{ in others}) \end{aligned} \tag{12}$$

As the largest component and other components have $\Theta(n)$ and $O(\log n)$ nodes, respectively, we can get

$$\mathbb{P}(E_k | g^* \text{ in others}) = o(\mathbb{P}(E_k | g^* \text{ in } G_p(n,k))).$$

Then, we further obtain from (12) that

$$\begin{aligned} \mathbb{P}(E_k) = \mathbb{P}(E_k | g^* \text{ in } G_p(n,k))\mathbb{P}(g^* \text{ in } G_p(n,k)) + \\ o(\mathbb{P}(E_k | g^* \text{ in } G_p(n,k))\mathbb{P}(g^* \text{ in } G_p(n,k))). \end{aligned} \tag{13}$$

Here, we only consider the $\beta \geq 1$ case as $\beta = 0$ indicates the trivial independent case. When the generator g^* is in the $G_p(n,k)$ component, there will be $a\beta n$ cyber nodes that still have the power according to the 1-β interdependence. This indicates that the random graph $G_c(k)$ devolves to at most $a\beta n$ cyber nodes forming a potentially connected graph in the cyber domain. Similarly, from the random graph property, there exists the largest component in $\mathcal{G}_c(k)$ with $G_c(a\beta n, k)$ cyber nodes satisfying that a.a.s.,

$$G_c(a\beta n, k) = \begin{cases} ba\beta n & q(a\beta n, k)a\beta n = c_c > 1 > a > 0 \\ a\beta n & q(a\beta n, k)a\beta n > \log n, \end{cases}$$

where $q(a\beta n, k)$ satisfies

$$q(a\beta n, k) = \frac{\beta n(\beta n + 1)q(n, 0) - k}{\beta n(\beta n + 1)}$$

The probability that the source cyber node to report the failure information is in $G_c(a\beta n, k)$ can be written as $G_c(a\beta n, k)/(\beta n)(1 - o(1))$.

1) When $q(a\beta n, k)a\beta n > \log n$:

1.1) under the interdependence-aware control policy, the destination cyber node always has the power. We have

$$\mathbb{P}(E_k | g^* \text{ in } G_p(n, k)) = a(1 - o(1)). \tag{14}$$

Combining (7), (11), (13), and (14) yields

$$\mathbb{P}(S_k) = a(1 - o(1))\mathbb{P}(d_k < D_k). \tag{15}$$

1.2) under the blind control policy, the destination cyber node always has the power with probability $G_c(a\beta n, k)/(\beta n)$. Then, we obtain $\mathbb{P}(E_k | g^* \text{ in } G_p(n, k)) = a^2(1 - o(1))$ and

$$\mathbb{P}(S_k) = a^2(1 - o(1))\mathbb{P}(d_k < D_k). \tag{16}$$

We let $\eta = a$ and $\theta = 1$ for interdependence-aware control; and let $\eta = a$ and $\theta = a$ for blind control.

2) When $q(a\beta n, k)a\beta n = c_c > 1 > a > 0$:

2.1) under the interdependence-aware control policy, we have $\mathbb{P}(E_k | g^* \text{ in } G_p(n, k)) = ab^2(1 - o(1))$ and and

$$\mathbb{P}(S_k) = ab^2(1 - o(1))\mathbb{P}(d_k < D_k) = \eta(1 - o(1)). \tag{17}$$

2.2) under the blind control policy, it holds that $\mathbb{P}(E_k | g^* \text{ in } G_p(n, k)) = a^2b^3(1 - o(1))$, and

$$\mathbb{P}(S_k) = a^2b^3(1 - o(1))\mathbb{P}(d_k < D_k). \tag{18}$$

In this case, we let $\eta = ab^2$ and $\theta = 1$ for interdependence-aware control; and let $\eta = ab^2$ and $\theta = ab$ for blind control. Combining the results in cases 1) and 2) completes the proof.

IV. System-level Simulations

In this section, we set up a smart grid system to perform comprehensive simulations to validate our theoretical analysis and evaluate how failures propagate with practical power system configurations under different interdependence models and control policies. We first describe our simulation system configurations and then present the results.

A. Simulation System Configurations

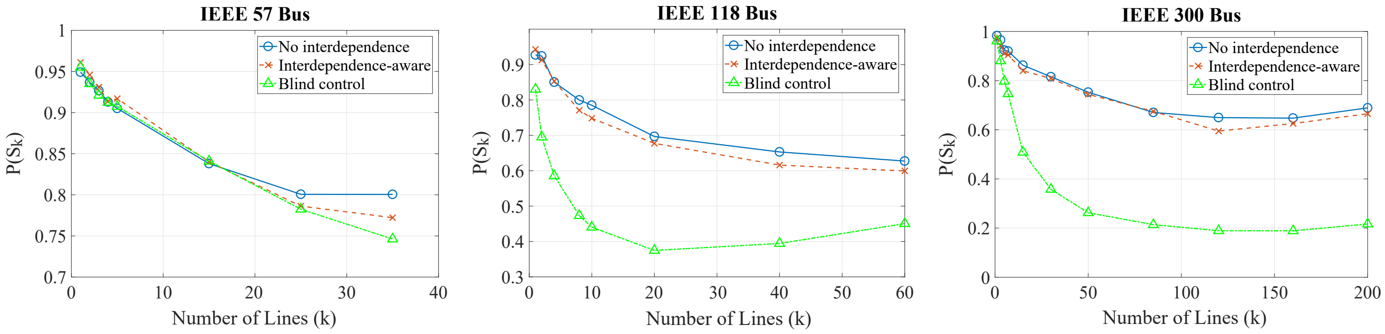
The physical domain of the smart grid has three standard power system topologies: IEEE 57-bus, 118-bus and 300-bus systems [24], which contain 80, 186 and 411 transmission lines, respectively. They are three widely-adopted power system stereotypes for power engineering research. More specifically, we configure the smart grid as follows.

- The physical domain: The IEEE 57-bus, 118-bus and 300-bus system topologies are adopted as the underlying power infrastructures. The capacity of each transmission line is set to be 1.1 times of its ordinary value, i.e., the value of power flow before any failure occurs in the power system. To calculate power flow, we adopt the Direct Current (DC) power flow model, which has been widely used in existing cascading failure studies [5], [14].
- The cyber domain: we build a communication network with the same topology as the physical domain. The random communication delay between each link is exponentially distributed, which is widely-used in the literature [15], [25], [26]. We choose the average link delay to be 0.1 ms, which has been demonstrated to yield good performance in stopping failure propagation [15]. The shortest path routing is used in the network.
- Interdependence: we adopt 1-0 and 1-1 interdependence models in simulations. The 1-0 model indicates that the communication network always has backup power supplies; and the 1-1 model means that one cyber node depends on one physical node, and vice versa.
- Control policy: we use the blind control and interdependence-aware control as discussed extensively in previous sections.
- Triggering failure: The initial failure is automatically triggered by randomly removing a power line in the physical domain when a simulation starts.

B. Simulation Result

Fig. 6 shows the simulation results of $\mathbb{P}(S_k)$ as functions of k under different interdependence and control policies with a physical domain being (a) IEEE 57-bus, (b) IEEE 118-bus, and (c) IEEE 300-bus systems. As $\mathbb{P}(S_k)$ denotes the probability that the failure propagation stops given the fact that k power line failures already happen, a higher value of $\mathbb{P}(S_k)$ indicates a better performance of load shedding control against failure propagation.

We first look at Fig. 6(a) showing the values of $\mathbb{P}(S_k)$ for three different control cases: (i) load shedding control under no cyber-physical interdependence ($\beta = 0$), (ii) interdependence-aware control under 1-1 interdependence, and (iii) blind control under 1-1 interdependence in the smart grid based on the IEEE 57-bus power system. It is very evident in Fig. 6(a) that during initial failure accumulation, the three cases lead to the similar values of $\mathbb{P}(S_k)$, indicating that the control effectiveness is not very sensitive to the control policy or the cyber-physical interdependence model. As the failure progresses (i.e., as the number of failed lines k increases), the



(a) IEEE 57-bus based system.

(b) IEEE 118-bus based system.

(c) IEEE 300-bus based system.

Fig. 6: Performance comparison of control under no interdependence, and interdependence-aware control and blind control under 1-1 interdependence in IEEE 57-bus, 118-bus and 300-bus based system.

control with no interdependence outperforms interdependence-aware control and blind control under 1-1 interdependence. This shows that interdependence comes into play and can degrade the effectiveness of failure mitigation. In this regard, interdependence-aware control is more effective than blind control because it makes decisions by considering failures of cyber nodes.

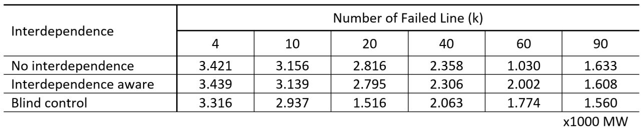
Similar to Fig. 6(a), Figs. 6(b) and (c) show the values of $\mathbb{P}(S_k)$ under the three control cases in the smart grids built upon IEEE 118-bus and IEEE 300-bus systems, respectively. We observe that each figure exhibits the similar two-phase phenomenon: during the initial failure accumulation, the values of $\mathbb{P}(S_k)$ are not very sensitive to the control policy or the interdependence model; during the steady failure propagation phase, blind control yields evidently smaller values of $\mathbb{P}(S_k)$ than the interdependence-aware control and non-interdependence cases.

The simulation results in Fig. 6 demonstrate the validity of theoretical analysis on the two-phase transition during load shedding control against failure propagation. During initial failure accumulation, we can conclude that improving the communication network performance and enhancing the power line capacity are among the most effective ways to improve the control effectiveness. During the steady failure propagation phase (particularly in Figs. 6(b) and (c)), if we compare the values of $\mathbb{P}(S_k)$ between the non-interdependence case and the interdependence-aware control case, we see approximately a constant degradation of $\mathbb{P}(S_k)$. In addition, the degradation from interdependence-aware control to the blind control case is also approximately a constant. These two constants are characterized by η and θ in Theorem 2. From Fig. 6, we note that interdependence-aware control must be used to improve the control effectiveness if cutting interdependence is not an option due to its cost of system deployment.

We also compare the amounts of left loads after k power line failures (also known as the *yields*) for the three control cases. We present the yields as functions of k in Table II from the IEEE 118-bus system simulation results.

From Table II, we can observe that the yields have the similar characteristics to $\mathbb{P}(S_k)$. When the number of failed lines is small, such as $k = 4$, the differences among the three cases are negligible. The differences gradually increase as k becomes larger. For example, when $k = 20$, the maximum difference between the yields is 300 megawatts (MW). Overall, we can see from Table II that blind control loses much more loads compared with interdependence-aware control and control under no interdependence, because it is not effective in mitigating failure propagation as shown in Fig. 6.

TABLE II: Comparisons of the amounts of shed loads between the three cases.



Interdependence	Number of Failed Line (k)					
	4	10	20	40	60	90
No interdependence	3.421	3.156	2.816	2.358	1.030	1.633
Interdependence aware	3.439	3.139	2.795	2.306	2.002	1.608
Blind control	3.316	2.937	1.516	2.063	1.774	1.560

x1000 MW

The simulation results based on IEEE 57-bus, 118-bus and 300-bus systems effectively characterize failure propagation in interdependent smart grid systems with realistic communication network and power system configurations.

V. Related Work

In the literature, the studies on understanding the positive and negative influences of the cyber-physical integration are conducted separately.

1) The Positive Side for Cyber-Physical Integration: Regarding how a communication network assists in mitigating cascading failures, many studies focused on modeling and characterizing cascading failures. A series of cascading failure models have been developed in the literature [5], [27]. A recent work [14] also explored geological correlations between consecutive failures during the failure propagation phase. Furthermore, there are also a number of studies trying to find the optimal load shedding solutions [4], [28] that minimize the load shedding cost while maximizing the served loads in the power grid. Many papers assumed that a perfect communication network exists to support information exchange with zero communication delay, which is not true in real-world systems. Although a recent paper [15] identified that poor communication performance can cause negative impacts on preventing failure propagation. An underlying assumption for all these studies is that there is a communication network independent of the power grid.

2) The Negative Side for Cyber-Physical Integration: On the other hand, research efforts have also been devoted to understanding how the interdependence due to cyber-physical integration may exacerbate a cascading failure in the smart grid. For example, in [8]–[10], cyber-physical interdependence models were built to characterize the scenarios, in which the communication network depends on the power grid for power supply; and at the same time, the power grid relies on the communication network for information exchange. As a result, the power grid failure can cause the communication network failure, and vice versa. The work in [6] studied a practical power grid and communication network in Italy, based on which a unidirectional and 1-to-many interdependent network model was developed. However, the realistic impact of the communication network on the control of the power grid is not explicitly specified in the work.

A common drawback in most existing interdependent network studies is that the interdependence between the communication network and the power system is simplified to node-to-node relationship; i.e., the failure of a node in one domain can lead to the failure of the corresponding node in another domain. Our failure model in this paper is much more realistic than existing works because we consider the realistic connectivities in the cyber and physical domain graphs to determine the failures of cyber and physical edges under the 1-β interdependence model, while also allowing $\beta = 0$ to indicate the non-interdependence case.

VI. Conclusions

In this paper, we developed a systematic framework to model and analyze the impact of cyber-physical interdependence on the failure mitigation process. We revealed both positive and negative sides of cyber-physical integration: during initial failure accumulation, the performance of the integrated communication network is a dominant factor for helping load shedding control to mitigate the failure propagation; however, during steady failure propagation, the interdependence in such integration comes into play and can substantially degrade the effectiveness of failure mitigation. Finally, we used system-level simulations to evaluate the impact of cyber-physical interdependence on the failure mitigation process based on IEEE standard power systems.

Acknowledgment

Dr. Zhuo Lu was supported in part by ONR N000141712109 and FC2 2017 seed grant.

Dr. Xiang Lu was supported in part by NSFC 61402476.

References

[1] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, pp. 18–28, 2010.

[2] M. IEEE PES CAMS Task Force on Understanding, Prediction and R. of Cascading Failures, "Initial review of methods for cascading failure analysis in electric power transmission systems," in *Proc. of IEEE PES General Meeting*, July 2008, pp. 1–8.

[3] ——, "Risk assessment of cascading outages: methodologies and challenges," vol. 27, no. 2, May 2012, pp. 631–641.

[4] D. Xu and A. A. Girgis, "Optimal load shedding strategy in power systems with distributed generation," in *Power Engineering Society Winter Meeting, 2001. IEEE*, vol. 2. IEEE, 2001, pp. 788–793.

[5] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, 2007.

[6] V. Rosato, L. Issacharoff, F. Tiriticco *et al.*, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1-2, pp. 63–79, 2008.

[7] H. Xiao and E. M. Yeh, "Cascading link failure in the power grid: A percolation-based analysis," in *Proc. IEEE ICC*, 2011.

[8] M. Parandehgheibi and E. Modiano, "Robustness of interdependent networks: The case of communication networks and the power grid," in *Proc. of IEEE GLOBECOM*, 2013.

[9] M. Parandehgheibi, E. Modiano, and D. Hay, "Mitigating cascading failures in interdependent power grids and communication networks," in *Proc. IEEE SmartGridComm*, 2014.

[10] W. K. Chai, V. Kyritsis, K. V. Katsaros, and G. Pavlou, "Resilience of interdependent communication and power distribution networks against cascading failures," in *Proc. IFIP Networking*, 2016.

[11] S. T. Egbert, "Raising the bar on substation backup power," *Power Grid International*, vol. 10, 2005.

[12] G. Wright, "Substation batteries: The key to reliability," *T&D World Magazine*, 2013.

[13] B. Liscouski and W. Elliot, "Final report on the august 14, 2003 blackout in the united states and canada: Causes and recommendations," *A report to US Department of Energy*, vol. 40, no. 4, 2004.

[14] A. Bernstein, D. Bienstock, D. Hay *et al.*, "Power grid vulnerability to geographically correlated failures - analysis and control implications," in *Proc. IEEE INFOCOM*, 2014.

[15] Z. Lu, M. Wei, and X. Lu, "How they interact? understanding cyber and physical interactions against fault propagation in smart grid," in *Proc. IEEE INFOCOM*, May. 2017.

[16] P. Palensky and D. Dietrich, "Demand side management: Demand response, intelligent energy systems, and smart loads," *IEEE Trans. Industrial Informatics*, vol. 7, pp. 381–388, 2011.

[17] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. Hines, "Dynamic modeling of cascading failure in power systems," *IEEE Trans. Power Systems*, vol. 31, no. 3, pp. 2085–2095, May 2016.

[18] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Trans. Power Systems*, vol. 30, no. 1, pp. 285–297, 2015.

[19] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *EPJB-Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.

[20] E. W. Zegura, K. L. Calvert, and M. J. Donahoo, "A quantitative comparison of graph-based models for internet topology," *IEEE/ACM Trans. Networking*, vol. 5, no. 6, pp. 770–783, 1997.

[21] Q. Chen, H. Chang, R. Govindan, and S. Jamin, "The origin of power laws in internet topologies revisited," in *Proc. IEEE INFOCOM*, 2002.

[22] M. Haenggi, J. G. Andrews, F. Baccelli *et al.*, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 7, 2009.

[23] B. Bollobas, *Random graphs*. Cambridge University Press, 2001.

[24] Power Systems Test Case Archive. [Online]. Available: https://www.ee.washington.edu/research/pstca/

[25] R. Nelson, *Probability, stochastic processes, and queueing theory: the mathematics of computer performance modeling*. Springer Science & Business Media, 2013.

[26] Y. Wang, M. C. Vuran, and S. Goddard, "Cross-layer analysis of the end-to-end delay distribution in wireless sensor networks," *IEEE/ACM Trans. Networking*, vol. 20, pp. 305–318, 2012.

[27] J. Chen, J. S. Thorp, and I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power & Energy Systems*, vol. 27, no. 4, pp. 318–326, 2005.

[28] W. Luan, M. R. Irving, and J. S. Daniel, "Genetic algorithm for supply restoration and optimal load shedding in power system distribution networks," *IEE Proceedings-Generation, Transmission and Distribution*, vol. 149, no. 2, pp. 145–151, 2002.