How They Interact? Understanding Cyber and Physical Interactions against Fault Propagation in Smart Grid

Zhuo Lu
Department of Electrical Engineering
University of South Florida
Tampa FL 33620
Email: zhuolu@usf.edu

Mingkui Wei
Department of Computer Science
Sam Houston State University
Huntsville, TX 77341
Email: mwei@shsu.edu

Xiang Lu
Institute of Information Engineering
Chinese Academy of Sciences
Beijing 100093, China
Email: luxiang@iie.ac.cn

***Abstract*—In the smart grid, computer networks (i.e., the cyber domain) are built upon physical infrastructures (i.e., the physical domain) to facilitate advanced functionalities that were considered not possible in legacy systems. It is envisioned that such a cyber-physical paradigm enables intelligent, collaborative controls to prevent faults from propagating along large-scale infrastructures, which is a primary cause for massive blackouts (e.g., Northeast blackout of 2003). Despite this promising vision, how effective cyber and physical interactions are against fault propagation is not yet fully investigated.**

In this paper, we use analysis and system-level simulations to characterize such interactions during load shedding, which is a process to stop fault propagation by shedding a computed amount of loads based on collaborative communication. Specifically, we model faults happening in the physical domain as a counting process, with each count triggering a load shedding action on the fly in the cyber domain. We show that although global load shedding design is considered optimal by globally coordinating shedding actions in power engineering, its induced failure probability (defined as the one that at least a given number of power lines fail) is scalable to the delay performance and the system size in the cyber domain, thus less likely to stop fault propagation in large systems than local shedding design that sheds loads within a limited system scope. Our study demonstrates that a joint view on cyber and physical factors is essential for failure prevention design in the smart grid.

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

I. Introduction

The smart grid [1] has become one of the most representative cyber-physical systems, in which computer networks (i.e., the cyber domain) are built upon physical infrastructures (i.e., the physical domain) to enable intelligent control functionalities. Bringing networking into the power grid [2], [3] is envisioned to make physical infrastructures more resilient and robust against fault propagation [4]–[8], which is a primary cause for a number of largest blackouts in history, such as the Northeast blackout of 2003 [9].

In power engineering, a power line has its capacity to transmit the power. If the power exceeds the capacity, the power line will become overloaded and have a chance to fail (i.e., be damaged and disconnected from the network due to overload), which is called as a fault or a failure. Such a fault disconnects a power line and accordingly leads to immediate power flow redistribution across the network, which can in turn overload other power lines and cause them to fail, and eventually become an unstoppable fault propagation event, also known as a cascading failure [6], [7], [10]. The initial fault or disconnection of a power line can be caused by accidents, human errors or nature events (e.g., lightening striking).

To rescue a power system from such a cascading failure, load shedding [4], [11]–[13] has been developed as an effective countermeasure. The basic idea of load shedding is straightforward: when a fault event is detected, a number of loads will be intentionally shed to eliminate the overload in the system, thereby stopping the fault propagation. In legacy power systems, the load shedding design is both empirical and heuristic. There is no guarantee that one shedding definitely makes no line be overloaded. Therefore, once a device detects a failure, it will shed a set of loads with pre-computed amounts gradually with attempt to halt the failure propagation eventually [11], [14], which is called local load shedding.

With the advent of the smart grid technology, global load shedding has been proposed as the optimal solution [4], [15] for stopping fault propagation, in which a control center collects all system information and uses a global optimization framework to shed the optimal amount of loads for making the system re-balanced without overload and at the same time keeping the cost minimum (thus ensuring the minimum number of clients losing the power). The cyber domain is the essential medium for information exchange in global load shedding: the control center collects failure information then sends load shedding commands to corresponding devices to execute in the physical domain. Existing studies [4], [15] always assume that information exchange finishes instantly (i.e., without delay). However, the assumption never holds in practice due to randomness (e.g., random delay and retransmissions) in communication networks. Moreover, from reliability and security perspectives, this assumption is risky because it gives a false sense that a protective procedure in the physical domain can fully rely upon an infrastructure in the cyber domain, which is nonetheless imperfect, and has shown vulnerabilities to various malicious cyber attacks in the real world [16]–[19].

From a practical view on an imperfect cyber domain, fault propagation under load shedding in fact constitutes a cyber-physical interactive process with actions affecting each other.

However, there is no systematic study in the literature on how this interactive process works to prevent fault propagation. In this paper, we take a combined analytical and experimental approach to model and evaluate the interactive process induced by fault propagation under load shedding. In particular, we model the number of power line failures in the physical domain as a counting process $\{M(t); t \geq 0\}$, where the initial triggering failure happens at time $t = 0$. Each count in $\{M(t); t \geq 0\}$ triggers another process in the cyber domain representing the delay of a load shedding action that will be eventually acted on the physical domain. We characterize the effectiveness of the cyber-physical interactions using the probability that at least m power lines fail eventually after the fault propagation, called as the failure probability denoted by $\mathsf{P}(M(\infty) \geq m)$. We use both analysis and system-level simulation experiments to understand how $\mathsf{P}(M(\infty) \geq m)$ is affected by the imperfect cyber domain. Our findings and contributions can be summarized as follows

- We take a combined approach based on analytical modeling and system-level simulations to characterize the interactions between cyber and physical domains during the load shedding procedure against fault propagation in the smart grid.
- We find that under global load shedding, the failure probability $\mathsf{P}(M(\infty) \geq m)$ is bounded from below by an increasing function of the number of nodes in a smart grid system; and the performance of global load shedding does not scale well with the number of nodes, especially when the cyber domain adopts wireless networking.
- Although recent studies embrace global load shedding in the smart grid and consider local load shedding legacy, our results reveal that local shedding can perform better than global shedding in the presence of a practical cyber domain. The results encourage a hybrid load shedding solution that combines local and global schemes.

To the best of our knowledge, we are the first to formally characterize the cyber-physical interactions during fault propagation under load shedding in the smart grid. Our results further indicate that although bringing communication networking into power grids is a significant leap forward and makes intelligent controls feasible, substantial efforts are still needed to make them from feasible to practically efficient by joint design across both domains, instead of limiting the design scope in one domain while assuming the ideal case in another.

The rest of the paper is organized as follows. In Section II, we introduce the models and state our research problems. In Section III, we present analytical results and their indications in practical design. In Section IV, we discuss the results from simulation experiments. In Section V, we present related work. Finally, we conclude this paper in Section VI.

II. Backgrounds, Models and Problem Statement

In this section, we introduce backgrounds, define basic models, and finally state our research problems.

A. The Smart Grid and Network Architecture

In the smart grid [2], [3], [12], a node representing a power or computing device may have a physical connection to the power infrastructure and a cyber connection to the communication network. We model such a system by a multigraph that is a graph whose nodes are allowed to have parallel edges. In our settings, the smart grid is denoted as $\mathcal{G} = (\mathcal{N}, \mathcal{E}_c, \mathcal{E}_p)$, where $\mathcal{N}$ is the set of all nodes, $\mathcal{E}_c$ and $\mathcal{E}_p$ are the sets of cyber and physical edges, respectively. We call the power system graph $\mathcal{G}_p = (\mathcal{N}, \mathcal{E}_p)$ the physical domain, and call the cyber system graph $\mathcal{G}_c = (\mathcal{N}, \mathcal{E}_c)$ the cyber domain. They can be both considered as subgraphs of the multigraph $\mathcal{G} = (\mathcal{N}, \mathcal{E}_c, \mathcal{E}_p)$. The physical edge represents the physical power connection in the physical domain $\mathcal{G}_p$ and the cyber edge denotes the cyber connection enabled by any communication networking technology in the cyber domain $\mathcal{G}_c$.

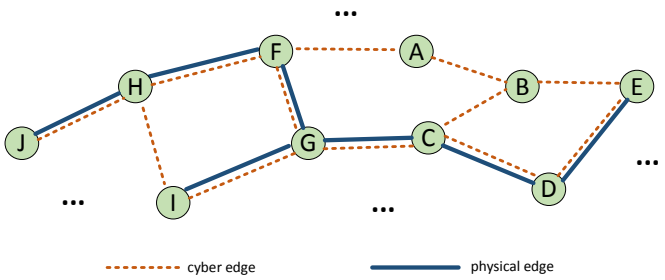

Fig. 1. An example of a smart grid system modeled by a multigraph with physical and cyber edges.

In the smart grid $\mathcal{G} = (\mathcal{N}, \mathcal{E}_c, \mathcal{E}_p)$, a node $v \in \mathcal{N}$ can denote any electronic device, such as power flow sensor, intelligent electronic device (IED), or communication device. We assume that there exist at most two edges of different types between two nodes in $\mathcal{N}$. Fig. 1 illustrates an example of a smart grid system modeled by a multigraph. As shown in Fig. 1, nodes C and D have both physical and cyber edges, and nodes A and B are connected by only one cyber edge.

B. Fault Propagation in the Physical Domain

In the physical domain $\mathcal{G}_p$, a fault or failure event can happen when there is a short circuit or overheat on a power line (i.e., a physical edge in $\mathcal{G}_p$) due to accidents, human errors or natural disasters [5], [6], [20]. When the power line fails, it is disconnected from the system. Such a disconnection in turn leads to power flow redistributed on the rest power lines, which, however, increases the loads on some other power lines. If the increased load due to the redistributed power flow on a line exceeds its capacity, the line will become unstable, and start to fail, and finally be disconnected from the system. This inevitably results in power redistribution and failures again, eventually becoming a cascading failure process [6], [7], [9] over the entire physical domain $\mathcal{G}_p$.

According to existing study in power engineering [4], [5], fault propagation in power grids cannot be exactly characterized by correlated failure models widely used in the communication network research, in which a node's neighbors

usually fail following the failure of the node [21], [22]. Rather, failure propagation in power grids depends on how the power flow is redistributed on other lines and the capacities of those lines. This indicates that when a line fails, its neighbor lines do not necessarily fail. Instead, a line that is far away can fail as long as more power is redistributed to flow on it and exceeds its capacity [4].

In this paper, we assume that the initial fault happens on a physical edge at time $t = 0$, triggering the failure propagation in the physical domain $\mathcal{G}_p$. It can be expected that as time t goes, more and more lines may fail and be disconnected from the physical domain $\mathcal{G}_p$. We aim to measure the potential scale of the failure propagation. We first define the total number of failed lines over time t as the following process.

Definition 1: The total number of failed lines $\{M(t); t \geq 0\}$ over time t is an inhomogeneous counting process with the i-th random counting interval τ_i depending on i.

The inhomogeneity of τ_i (i.e., its dependence on i) is used to characterize the fact that a line may fail at a different rate after each time a failure happens and the power flow is redistributed in the network. Based on Definition 1, we use the following failure probability to measure the eventual scale of fault propagation in the physical domain $\mathcal{G}_p$.

Definition 2: The failure probability is defined as the probability that at least m power lines eventually fail in the physical domain $\mathcal{G}_p$ and is written as $\mathsf{P}(M(\infty) \geq m)$.

When there is no protective procedure to stop fault propagation, we can expect that $\mathsf{P}(M(\infty) \geq m)$ can be close to 1 for a reasonably large m.

C. Load Shedding in the Cyber Domain

Unstoppable fault propagation can cause devastating impacts on power grids, leading to massive blackouts over large areas. To stop fault propagation, load shedding [4], [11]–[13] has been proposed as an effective measure, in which a number of loads will be shed to ensure that the redistributed power will not exceed the capacity of any remaining line in the physical domain $\mathcal{G}_p$. The cost of load shedding is that some clients have to be disconnected from the power grid.

Load shedding can be performed at a local or global level.

- Load shedding in legacy power grids works in a preset way [14]; i.e., when a system detects a fault, some prechosen loads will be shed in turn with attempt to prevent fault propagation, which is usually not optimal in terms of both effectiveness and cost. In this paper, we called this way *local load shedding* as it is preset and does not need global information.
- In the smart grid scenario, a load shedding algorithm is designed to be smart such that it computes how to shed in the physical domain $\mathcal{G}_p$ the minimum amount[1] of loads to stop fault propagation. This effectively halts a cascading failure event and at the same time ensures minimum blackouts among clients [4]. During this process, a control center and a number of nodes actively communicate with one another in the cyber domain $\mathcal{G}_c$ to ensure successful load shedding in the physical domain $\mathcal{G}_p$. Based on global information, the algorithm guarantees the optimal solution; i.e., it ensures shedding the minimum loads (thereby disconnecting the minimum number of clients) to stop a massive blackout. We call such an algorithm *global load shedding*.

Global load shedding has gained attention as it is considered as the optimal solution in power engineering [4], [15]. However, global load shedding does depend on messaging among nodes and the control center in the cyber domain $\mathcal{G}_c$ to prevent fault propagation in the physical domain $\mathcal{G}_p$. The effectiveness of computer networking therefore becomes the key for a successful load shedding. In smart grid settings, such an effectiveness is generally measured by the delay metric instead of the throughput metric [3], [16]. Thus, we define the action delay of load shedding as follows.

Definition 3: The action of load shedding is triggered at each epoch (i.e., the time instant that the count changes) in the process $\{M(t); t \geq 0\}$ with delay d_i in the cyber domain $\mathcal{G}_c$ to denote the duration between the time that the i-th load shedding procedure starts and the time that the corresponding load is shed in the physical domain $\mathcal{G}_p$.

We assume that an action with scope limited in the physical domain, such as detecting failures and shedding loads, takes a constant delay, which can be subtracted accordingly from $\{\tau_i\}$, and therefore does not affect stochastic analysis. In this way, the action delay d_i becomes the delay in the cyber domain $\mathcal{G}_c$ to deliver load shedding information after i-th line fails.

D. Problem Statement

After introducing necessary backgrounds and defining the performance metric, we aim to address the following two research questions in this paper.

- How to formulate and characterize the failure probability $\mathsf{P}(M(\infty) \geq m)$?
- What are the most important factors to use global and local load shedding to stop failure propagation?

We will focus on using both analytical modeling and system-level simulations to study the research problems.

III. Analytical Formulation and Results

In this section, we investigate the research problems by developing our formulation and analysis strategies, and present the results.

A. Analyzing Cyber and Physical Interactions during Fault Propagation under Load Shedding

After a fault happens in the physical domain $\mathcal{G}_p$, more and more lines may start to fail due to overload if there is no strategy to prevent such failures. Existing studies [4]–[6], [20], [23], [24] have shown that fault propagation along power infrastructures is a complicated process. It depends on where the initial fault is, the power network topology, power loads and capacities of power lines. Analytical results on how faults exactly propagate are mathematically intractable. As

[1]More formally, the goal of global load shedding is to keep a cost metric minimum. In this paper, we use the amount of loads as the cost.

a result, simulation approaches are generally adopted in the power engineering community [4], [5]. On the other hand, analytical approaches based on simplified connectivity models are investigated in the complex network community [23], [24]. All these studies only focus on the physical domain instead of jointly considering both cyber and physical domains.

When communication-enabled load shedding comes into play, the fault propagation in the system can be stopped when sufficient loads are shed. During the whole process of a load shedding procedure, except for the initial fault detection and the final shedding action in the physical domain $\mathcal{G}_p$, the major part of load shedding in fact resides in the cyber domain $\mathcal{G}_c$. That is, nodes must communicate with one another to decide how to shed, where to shed, and accordingly notify corresponding nodes of the load shedding actions. All of the information exchange happens in the cyber domain $\mathcal{G}_c$.

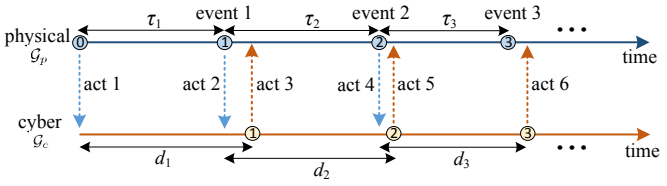

Fig. 2. Example of time events on cyber and physical domains and how they interact with each other during fault propagation under load shedding.

To offer an analytical formulation, we need to first clearly understand how the cyber and physical domains interact. Fig. 2 shows such an example from a timing perspective for modeling. Suppose in Fig. 2 that there is no cyber domain: when the initial triggering fault happens in the physical domain at time 0, the physical domain $\mathcal{G}_p$ becomes unstable and starts to redistribute power flows, which in turn leads to the first line failure[2] after a time duration of τ_1 (according to Definition 1), shown as event 1 in Fig. 2. Then, the second and third failures follow, denoted as events 2 and 3, respectively, in Fig. 2. As there is no protective procedure, the failure will eventually stop when a majority of power lines have failed.

Now suppose that the system adopts a load shedding strategy in the cyber domain $\mathcal{G}_c$ in Fig. 2: when the fault happens at time 0, this fault will be detected and reported via messages in $\mathcal{G}_c$ (as denoted by act 1 in Fig. 2) to necessary nodes (including the control center if there is one). When a decision is made, load shedding commands will be sent out via $\mathcal{G}_c$ to execute in $\mathcal{G}_p$. The entire process incurs a delay of d_1 in $\mathcal{G}_c$, as shown in Fig. 2. The failure will stop if $d_1 < \tau_1$, because the necessary load is shed to make the system re-balanced without overload. However, d_1 is a random action delay due to random traffic and random network protocols in $\mathcal{G}_c$. It may also happen that $d_1 > \tau_1$ as illustrated in Fig. 2. In this regard, the second line fails and further increases the overload in the system. This means that even when $\mathcal{G}_c$ lets $\mathcal{G}_p$ shed the computed load in act 3 in Fig. 2, it is not enough after the second failure; hence, the fault propagation continues.

[2]Note that we always exclude the initial triggering failure when we count the number of line failures in this paper.

It is also noted that when the second line fails, $\mathcal{G}_p$ also notifies $\mathcal{G}_c$ of such an event in act 2 shown in Fig. 2, which triggers the second load shedding operation with delay d_2. Unfortunately, the information delivery of the load shedding action is still not on time in $\mathcal{G}_c$, leading to the third failure in $\mathcal{G}_p$, and so on, as illustrated in Fig. 2.

B. Analytical Results and Discussions

Fig. 2 demonstrates that fault propagation under load shedding as an inhomogeneous counting process in the physical domain $\mathcal{G}_p$ coupled with a similar process in the cyber domain $\mathcal{G}_c$. Each process also depends on the physical or cyber network topology after each failure. It is mathematically intractable to characterize $\{M(t); t \geq 0\}$ and its associated failure probability $\mathsf{P}(M(\infty) \geq m)$ in exact closed-form analysis.

Our strategy is to characterize $\mathsf{P}(M(\infty) \geq m)$ in a generic formulation, and adopt an analytical lower bound analysis to predict theoretically how $\mathsf{P}(M(\infty) \geq m)$ is affected by the message delivery in the cyber domain. Then, we will use system-level simulations in the next section to validate the analysis and show more practical results with realistic cyber and power domain settings.

We first show that the failure probability $\mathsf{P}(M(\infty) > m)$ can be derived as follows.

Theorem 1: Given the physical and cyber interactions in Definitions 1 and 3, the failure probability $\mathsf{P}(M(\infty) \geq m)$ satisfies

$$\mathsf{P}(M(\infty) \geq m) = 1 - \sum_{l=1}^{m} (-1)^{l-1} \sum_{\{x_1,\cdots,x_l\} \in \mathcal{R}_{l,m}} \mathsf{P}\left(\bigcap_{k=1}^{l} \bigcap_{i=x_{k-1}}^{x_k} A_{i,x_k}^c \right), \tag{1}$$

where $\mathcal{R}_{l,m} = \{x_1, x_2, \cdots, x_l | 1 \leq x_1 \leq x_2 \cdots \leq x_l \leq m\}$, $x_0 = 1$, and event $A_{i,j}$ $(j \geq i \geq 1)$ represents the event that the j-th load shedding is acted in the physical domain after the i-th failure happens, satisfying

$$A_{i,j} = \left\{ d_i > \sum_{k=j}^{i} \tau_k \right\}. \tag{2}$$

Proof: To obtain $\mathsf{P}(M(\infty) \geq m)$, we take a close look at event $\{M(\infty) \geq m\}$, which represents that there are at least m failed lines (excluding the initial triggering failure) eventually in the physical domain. This in turn means that at least m load shedding actions happened in the cyber domain, but loads were not shed on time to prevent fault propagation. This can imply the case shown in Fig. 2 that each load shedding action is delayed and performed right after the next fault happens. This also includes some other cases shown in Fig. 3: (a) all actions were delayed, but some may be significantly delayed (e.g., $d_2 > \tau_2 + \tau_3$); (b) some action (e.g., $d_3 < \tau_3$) may arrive on time, but the others are not.

Event $A_{i,j}$ $(i \geq j \geq 1)$ denotes the event that the j-th load shedding is acted in the physical domain after the i-th failure happens. Then, $A_{1,1}$ means that the first load shedding is acted after the first failure happens, i.e., $d_1 > \tau_1$; $A_{1,2}$ means that the

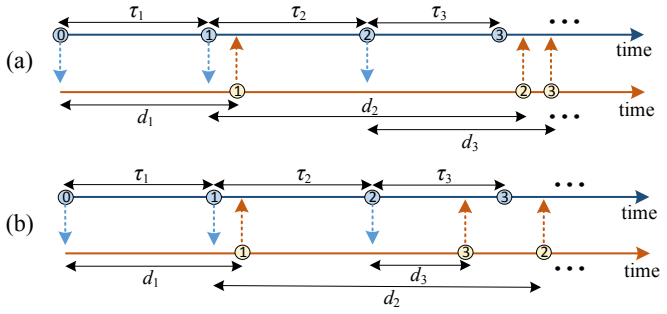

Fig. 3. Examples of how faults can keep propagating.

first load shedding is acted after the second failure happens, i.e., $d_1 > \tau_1 + \tau_2$; In general, we can obtain (2).

Let event B_i represent the event that i-th failure happens. Then, B_1 means that the first load shedding does not arrive before the first failure happens, therefore $B_1 = A_{1,1}$; B_2 means that B_1 happens (otherwise, there will be no second load shedding) and at the same time the first two load shedding actions do not arrive before the second failure happens, therefore $B_2 = B_1 \cap (A_{1,2} \cup A_{2,2}) = A_{1,1} \cap (A_{1,2} \cup A_{2,2})$, and $B_3 = B_2 \cap B_1 \cap (A_{1,2} \cup A_{2,2}) = A_{1,1} \cap (A_{1,2} \cup A_{2,2}) \cap (A_{1,3} \cup A_{2,3} \cup A_{3,3})$, and so on. By induction, we have

$$B_i = B_{i-1} \cap \bigcup_{j=1}^{i} A_{j,i} = \bigcap_{l=1}^{i} \bigcup_{j=1}^{l} A_{j,l}. \tag{3}$$

Thus, event $\{M(\infty) \geq m\}$ is equivalent to the event that at least m failures happen, i.e., B_m; and we have from (3)

$$\begin{aligned} &\mathsf{P}(M(\infty) \geq m) = \mathsf{P}(B_m) \\ &= \mathsf{P}\left(\bigcap_{l=1}^{m} \bigcup_{j=1}^{l} A_{j,l}\right) = 1 - \mathsf{P}\left(\bigcup_{l=1}^{m} C_l\right), \end{aligned} \tag{4}$$

where

$$C_l = \bigcap_{j=1}^{l} A_{j,l}^c. \tag{5}$$

According to the inclusion-exclusion principle [25], we can write (4) as

$$\mathsf{P}(M(\infty) \geq m) = 1 - \sum_{l=1}^{m} (-1)^{l-1} S_l, \tag{6}$$

where

$$\begin{aligned} S_l &= \sum_{1 \leq x_1 \leq x_2 \cdots \leq x_l \leq m} \mathsf{P}\left(\bigcap_{k=1}^{l} C_{x_k}\right) \\ &= \sum_{1 \leq x_1 \leq x_2 \cdots \leq x_l \leq m} \mathsf{P}\left(\bigcap_{k=1}^{l} \bigcap_{j=1}^{x_k} A_{j,x_k}^c\right) \\ &= \sum_{1 \leq x_1 \leq x_2 \cdots \leq x_l \leq m} \mathsf{P}\left(\bigcap_{k=1}^{l} \bigcap_{j=x_{k-1}}^{x_k} A_{j,x_k}^c\right), \end{aligned} \tag{7}$$

which completes the proof. □

Remark 1: Although Theorem 1 does not offer a closed-form solution to the failure probability, it gives a generic mathematical expression to compute the failure probability without specific assumptions on $\{d_i\}$ and $\{\tau_i\}$. In fact, it can be verified that the failure probability in (1) from Theorem 1 is an increasing function of d_i. This implies that the failure probability increases when the message delivery performance in the cyber domain $\mathcal{G}_c$ becomes worse, because the information delivery rate for load shedding is slowed down and may not always catch up with the fault propagation speed in the physical domain $\mathcal{G}_p$.

To show how exactly the delay performance affects the failure probability, we adopt additional assumptions for a lower bound analysis approach, which enables mathematical formulation to study the relations between $\mathsf{P}(M(\infty) \geq m)$ and $\{d_i\}$. In this way, we can understand that when the delay performance becomes an adverse factor, how it increases the lower bound of $\mathsf{P}(M(\infty) \geq m)$ and in turn exacerbates the fault propagation. Then, we will use simulations in the next section to validate the analysis and further show detailed results of fault propagation under load shedding with practical cyber and physical domain settings.

To proceed, we assume that the action delay of load shedding $\{d_i\}$ in the cyber domain $\mathcal{G}_c$ is exponentially distributed. Note that d_i is the time duration from the time that a fault is detected to the time that load shedding is acted in the physical domain $\mathcal{G}_p$. It represents the time duration for a number of message deliveries in the cyber domain $\mathcal{G}_c$, including notification of the failure detection and the delivery of load shedding commands. In essence, it can be considered as a sum of several message delays in a communication network. The exponential distribution is a widely-adopted model to facilitate analysis of link or path delay in a network [26], [27]. Mathematically, the sum of exponentially distributed random variables also exhibits an exponential tail. Therefore, We assume $\{d_i\}$ following the exponential distribution and state our result as follows.

Theorem 2: Denote by $n = |\mathcal{N}|$ the number of nodes in the network $\mathcal{G} = (\mathcal{N}, \mathcal{E}_c, \mathcal{E}_p)$. If load shedding delay d_i is exponentially distributed with mean denoted in the asymptotic notation as $\mathsf{E}(d_i) = \Theta(g(n))$ for some function $g(\cdot)$, and τ_i has a finite mean, it holds that

$$\mathsf{P}(M(\infty) > m) \geq e^{-\Theta\left(\frac{m f(\{\tau_i\})}{g(n)}\right)}, \tag{8}$$

where $f(\{\tau_i\})$ is a function for $\{\tau_i\}$.

Proof: The proof is partly based on that for Theorem 1. We start from (4). It is clear that $\bigcap_{l=1}^{m} A_{l,l} \subset \bigcap_{l=1}^{m} \bigcup_{j=1}^{l} A_{j,l}$. Therefore,

$$\begin{aligned} \mathsf{P}(M(\infty) \geq m) &\geq \mathsf{P}\left(\bigcap_{l=1}^{m} A_{l,l}\right) = \prod_{l=1}^{m} \mathsf{P}(A_{l,l}) \\ &= \prod_{l=1}^{m} \mathsf{E}(e^{-\lambda_i \tau_i}), \end{aligned} \tag{9}$$

where λ_i is the parameter for d_i satisfying $E(d_i) = 1/\lambda_i =$

$\Theta(g(n))$. Then, we further have,

$$\mathsf{P}(M(\infty) \geq m) \geq \prod_{l=1}^{m} \mathsf{E}(e^{-\lambda_i \tau_i}) = \prod_{l=1}^{m} \mathsf{E}\left(e^{-\frac{\tau_i}{\Theta(g(n))}}\right). \quad (10)$$

Because $e^{-\tau_i}$ is a convex function of τ_i, it follows from Jensen's inequality that

$$\mathsf{P}(M(\infty) \geq m) \geq \prod_{l=1}^{m} \mathsf{E}\left(e^{-\frac{\tau_i}{\Theta(g(n))}}\right) \geq \prod_{l=1}^{m} e^{-\frac{\mathsf{E}(\tau_i)}{\Theta(g(n))}}$$
$$= e^{\sum_{i=1}^{m}\left(-\frac{\mathsf{E}(\tau_i)}{\Theta(g(n))}\right)} = e^{-\Theta\left(\frac{m f(\{\tau_i\})}{g(n)}\right)}, \quad (11)$$

which finishes the proof. □

In Theorem 2, the average delay $\mathsf{E}(d_i)$ is denoted by an asymptotic function of the number of nodes n. According to the network scaling laws, such delay in the asymptotic notation exhibits distinct behaviors under different network architectures and protocols. This allows us to check the communication requirements of a load shedding design to analyze the induced failure probability.

For global load shedding design, in which the optimal amount of loads will be found and notified among the node set $\mathcal{N}$, the induced load shedding action delay depends on the end-to-end performance in the cyber domain $\mathcal{G}_c = (\mathcal{N}, \mathcal{E}_c)$. If the cyber domain $\mathcal{G}_c$ is a wireline network modeled as a random graph (e.g., Erdos-Renyi or small world [28]), its average length of end-to-end path is $\Theta(\log n)$, leading to $g(n) = \Theta(\log n)$. If the cyber domain $\mathcal{G}_c$ is a wireless network modeled as a random geometric graph, a typical end-to-end delay can be represented as $\Theta(\sqrt{n})$ [29], thereby $g(n) = \Theta(\sqrt{n})$.

Fig. 4 shows a numerical example to compare the lower bounds of the failure probability (computed from Theorem 2) under global load shedding between such wireline and wireless deployments in the cyber domain $\mathcal{G}_c$. We can observe in Fig. 4 that the lower bound of failure probability in the wireless network increases faster than the wireline network when n becomes large. This implies that although wireless networking has been widely proposed as a vital means to facilitate information exchange in the smart grid [3], [27], it is still less suitable for failure prevention than wireline networking in large-scale systems.

For local load shedding design, it only requires shedding a preset amount of loads in local deployments within limited scopes. Therefore, it only incurs a delay of $g(n) = \Theta(1)$, which leads to a lower bound in (8) not scaling with n. Comparing this bound with those due to global load shedding illustrated in Fig. 4, we conclude that interestingly, global shedding cannot be viewed as a uniformly better solution than local shedding when n is large, because the lower bound of failure probability due to global shedding scales with n .

Then, we move on to system-level simulations to validate theoretical predictions and characterize fault propagation process under load shedding with more detailed, practical settings.

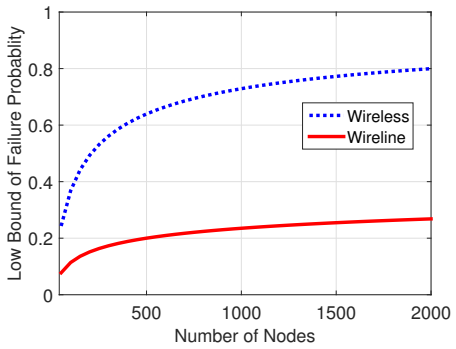

Fig. 4. Examples: the low bounds of the failure probability given a fixed $m = 100$ under global load shedding in wireless and wireline based cyber domains with average delays on the order of $\Theta(\sqrt{n})$ and $\Theta(\log(n))$, respectively.

IV. System-level Simulations

In this section, we set up a smart grid simulation system with practical settings to evaluate how faults propagate under load shedding. We first present setups and then discuss results.

A. System Configurations

1) Physical Domain: We use the IEEE 57-bus power system [30] as our physical domain in the system-level simulation. The 57-bus system represents a portion of the America Electric Power System in the Midwestern area, which contains 57 buses and 80 transmission lines with a total amount of loads being 1,250,800 kilowatts (KW). There are 4 power generators located at buses 1, 3, 8, and 12, respectively[3]. Based on the power injection (i.e., power generation or power consumption) at each bus, the power flow on each transmission line is calculated using the Direct Current (DC) power flow model in our simulations. While the Alternating Current (AC) power flow model provides more accurate approximation, it is not usually adopted in existing work [31] for fault propagation and load shedding studies due to its complexity.

2) Cyber Domain: In our initial setup, the cyber domain is a communication network with the same topology as the physical domain (i.e., the IEEE 57-bus system). In other words, each node in the simulated smart grid system assumes two roles: a power bus in the physical domain that connects power lines to a generator and/or loads, and an IED (installed on the bus) that monitors or controls its physical counterpart, and exchanges system operating information with the control center. We assume that the control center locates at bus 38, which is one of the buses that connects to the most buses. The communication network maintains routine system management traffic yielding a random link delay that can be configured in simulations.

3) Process of Fault Propagation under Load Shedding: In simulations, we set the capacity of each power line to be 1.1 times higher than the normal power flow value. The simulation randomly chooses one transmission line to fail and removes

[3]Due to the page limit, we do not show the IEEE 57-bus system architecture that is publicly available in [30].

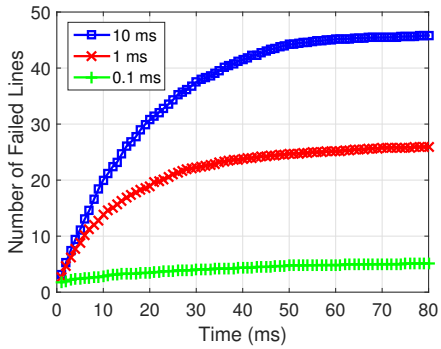

Fig. 5. The average number of failed lines over time with fault propagation under global load shedding. The average link delay is set to be 0.1 ms, 1 ms, or 10 ms.

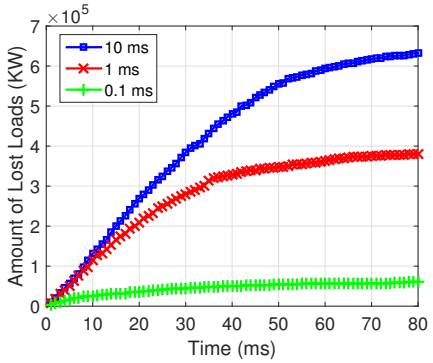

Fig. 6. The average amount of lost loads over time with fault propagation under global load shedding. The average link delay is set to be 0.1 ms, 1 ms, or 10 ms.

it from the system. This causes power redistribution in the physical domain, and in turn leads to more line failures and their removals from the system. Whenever a power line is overloaded and fails, the nodes that connect to both ends of the transmission line can detect this failure; and event messages are sent by both nodes to the control center. Based on the information, the control center will then calculate for a load shedding decision using a global load shedding algorithm in [4], [15]; and commands will be sent back to nodes to act accordingly. This process continues until at least one of the following conditions is met: (i) there is no overload in the system, and (ii) all lines that connect generators to loads have been disconnected, indicating a complete blackout.

For each simulation case, we capture the details of the failure event progressing at milliseconds (ms) level to obtain stable results.

B. Simulations and Results

We perform the following three major sets of simulations and present the results.

- Global load shedding with practical link performance. This is to measure how practical communication link performance in the cyber domain can affect the results of fault propagation under global load shedding.
- Global load shedding in wireline and wireless networks. As we have predicted in the previous section, the performance of global load shedding does not scale well with the number of nodes, especially in the wireless networks. This is to evaluate the performance with practical settings.
- Global vs. local load shedding. We aim to compare the effectiveness of global and local load shedding methods in a practical smart grid scenario.

1) Global Load Shedding with Practical Link Performance: Fig. 5 demonstrates the average numbers of failed lines over time with fault propagation under global load shedding. The average link delay varies from 0.1 ms to 10 ms; and Fig. 6 shows the average amounts of lost loads due to line failure associated with the same simulations in Fig. 5.

We can observe from Figs. 5 and 6 that when the average link delay is 10 ms, the average number of failed lines and the average amount of lost loads keep increasing over time, and eventually converge to 47 lines and $650,000$ KW, respectively. This means that even under global load shedding as a protective measure against fault propagation, the smart grid system still fails over half of its power lines and loses nearly half of its loads. Accordingly, the average link delay of 10 ms makes global load shedding less effective against fault propagation in the system. In this regard, a better communication quality in the cyber domain is needed.

Figs. 5 and 6 also show that when the average link delay becomes from 10 ms to 1 ms or 0.1 ms, the number of failed lines and the amount of lost loads are both significantly decreased. For example, when the average delay is 0.1 ms, the fault propagation eventually leads to 8 line failures and about $60,000$-KW loads lost on average. However, even when the link delay is very small in this case, we still observe that one line triggers more line failures in the physical domain. This is due to the randomness in the routine traffic pattern in the system, resulting in a small chance that load shedding messages are still delayed before more lines fail.

The results in Figs. 5 and 6 show that a better cyber domain enables global load shedding to be an effective way against fault propagation. On the other hand, however, Figs. 5 and 6 illustrate that even when the average delay is very small, it is still not safe to assume that load shedding messages can be delivered instantly. There always exists a small probability in the cyber domain to delay the delivery due to its randomness. As a consequence, we should always consider the random cyber domain factors in smart grid system design, rather than assuming perfection for the cyber domain.

2) Global Load Shedding in Wireline and Wireless Networks: Next, we evaluate the effectiveness of global load shedding in wireline and wireless networks. According to our prediction in Fig. 4, global load shedding does not scale well in large-scale wireless networks. To perform the simulation, we keep the physical domain unchanged, and add more nodes in the cyber domain for fine-grained monitoring. Both wireline and wireless networks use the shortest-path routing. The wireless network uses carrier sending multi-access with collision avoidance (CSMA/CA) as the multi-access protocol. When the

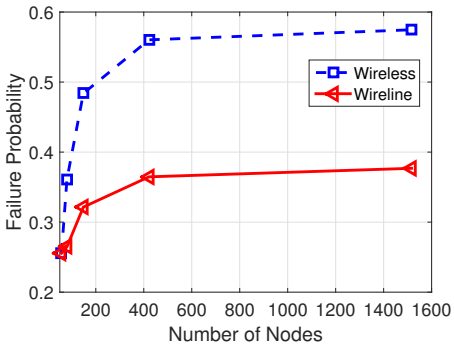

Fig. 7. The failure probability under global load shedding in wireless and wireline networks.

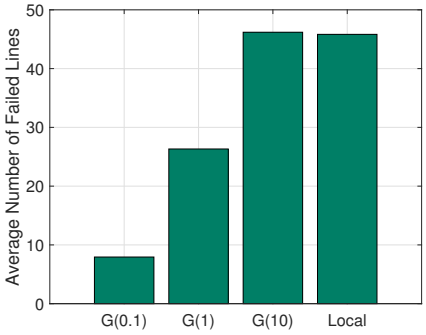

Fig. 8. The average numbers of failed lines under global and local load shedding schemes. G(0.1), G(1), and G(10) denote global load shedding with average link delay of 0.1 ms, 1 ms, and 10 ms, respectively.

number of nodes increases, the average link delay increases from 1 ms to around 5 ms and over 200 ms in wireline and wireless networks, respectively, due to more traffic loads and more collisions.

Fig. 7 measures the failure probability $\mathsf{P}(M(\infty) \geq m)$ with $m = 32$ (indicating that at least 32/80 = 40% of the lines in the physical domain fail) in simulated wireline and wireless networks, as a function of the number of nodes n. We can see that Fig. 7 exhibits curves similar to the theoretical predictions of the lower bounds in Fig. 4. In particular, it is noted that when the number of nodes increases, the failure probability increases to 0.38 and 0.57 for wireline and wireless networks, respectively. Hence, even though wireless networking is considered as a cost-efficient solution in the smart grid, it does not well support global load shedding in large networks. In this case, a higher wireless communication rate is needed to ensure a smaller failure probability, which unavoidably incurs more costs.

3) Global vs. Local Load Shedding: Finally, we compare the effectiveness between global and local load shedding schemes. In the local shedding scheme, we adopt a legacy way in which a number of loads are preset to shed; when a node detects a failure, it will immediately shed its preset loads without any communication.

Fig. 8 shows the average number of failed lines in the

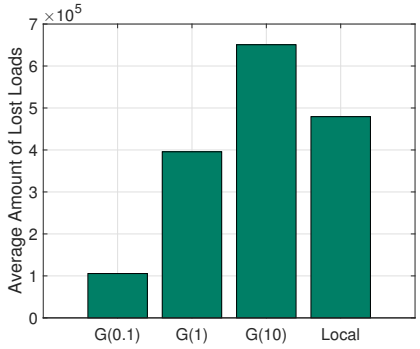

Fig. 9. The average amounts of lost loads under global and local load shedding schemes. G(0.1), G(1), and G(10) denote global load shedding with average link delay of 0.1 ms, 1 ms, and 10 ms, respectively.

system under global and local load shedding schemes. We can see that for global load shedding, when the average link delay increases, the total number of failed lines increases, indicating that the performance of global load shedding becomes worse. It is also observed from Fig. 8 that when the average link delay becomes 10 ms, global load shedding results in more failed lines than local load shedding. This reveals that global local shedding should only be considered optimal when the cyber domain sufficiently supports its actions.

Fig. 9 illustrates the average amount of lost loads with the same settings in Fig. 8. We can find in Fig. 9 that local load shedding is a much better solution than global load shedding when the average link delay becomes 10 ms. In this case, the benefit of load shedding over global shedding is over 130,000 KW, showing that local shedding becomes indeed better than global shedding when the cyber domain exhibits worse performance.

C. Discussions

In the following, we discuss the further observations and potential applications of our results: (i) Hybrid load shedding design. Although recent studies embrace global load shedding in the smart grid, our results show that local load shedding can still perform better than global load shedding in the presence of an imperfect cyber domain. This in fact suggests that interestingly, we should combine local and global schemes into a hybrid solution: when a node detects a fault event and also finds high delay in message delivery, it should act immediately to shed a preset amount of loads. This combined solution can partly cut the dependency of global load shedding on the cyber domain, which may not perform well in the presence of its own failures or malicious external attacks. (ii) Joint cyber-physical design. Our results show that the effectiveness of global load shedding is dependent on the performance of the communication network in the cyber domain. This indicates that in the interdisciplinary smart grid context, we should never solely design a solution within one domain while assuming that the another domain can perfectly support the design. A joint view of cyber-physical interactions is essential for any design involving both cyber and physical domains.

V. Related Work

Fault propagation, also known as cascading failure, has been studied in the literature. There are generally two approaches to characterize the impacts of fault propagation.

- Analytical modeling. This line of the work is generally based on a highly abstract complex or interdependent network model in relatively scientific settings (e.g., [6], [23], [24]), where a line failure is usually associated with a constant probability. The main objective is to analyze the eventual connectivity due to failures in the network. It is difficult to accommodate more practical power and communication factors into these models.
- Event or simulation based analysis approach. This approach has been widely adopted with a more practical view on realistic power engineering settings (e.g., [10], [11], [15]). Existing studies either analyze the historic events to understand how faults propagate, or use power system simulations to observe the impacts of fault propagation. Some studies (e.g., [5], [20]) also analyze the interdependence between the cyber and physical domains from a connectivity perspective, but without considering the performance factor in the cyber domain.

In the literature [4], [13]–[15], the load shedding design is mainly focused on developing an accurate optimization framework to stop the failure and minimize the cost, while assuming either implicitly or explicitly that the cyber domain can always support the design, which is not always guaranteed in practical smart grid scenarios. The research in this paper fills an important gap between existing results based on the perfect cyber domain assumption and practical smart grid scenarios with an imperfect cyber domain. We develop both analytical modeling and system-level simulation experiments to understand how the cyber and physical domains interact with each other under load shedding against fault propagation.

VI. Conclusions

In this paper, we provided a systematic study via analytical modeling and system-level simulations on characterizing cyber-physical interactions during fault propagation under load shedding in the smart grid. We found that the effectiveness of global load shedding is sensitive to the performance of the cyber domain: it does not scale well with the number of nodes, especially in wireless networks. We showed that local load shedding can perform better than global load shedding in the presence of an imperfect cyber domain. Our results encourage a hybrid load shedding solution and call for a joint view on cyber and physical domains for any design in the smart grid.

Acknowledgement

Zhuo Lu was supported in part by ONR N000141712109. 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] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - the new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 944–980, 2012.

[3] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, 2011.

[4] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures - analysis and control implications," in *IEEE INFOCOM*, 2014.

[5] 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 and Distributed Systems*, vol. 23, pp. 1708–1720, 2012.

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

[7] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Trans. Information Forensics and Security*, vol. 8, pp. 646–656, 2013.

[8] M. Wei and W. Wang, "Toward distributed intelligent: A case study of peer to peer communication in smart grid," in *IEEE GLOBECOM*, 2013.

[9] J. Minkel, "The 2003 Northeast blackout - five years later," *Scientific American*, vol. 13, 2008.

[10] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, pp. 1332–1336, 2009.

[11] P. Pourbeik, P. S. Kundur, and C. W. Taylor, "The anatomy of a power grid blackout," *IEEE Power & Energy Magazine*, vol. 4, 2006.

[12] M. Sechilariu, B. Wang, and F. Locment, "Building integrated photovoltaic system with energy storage and smart grid communication," *IEEE Trans. Industrial Electronics*, vol. 60, pp. 1607–1618, 2013.

[13] H. You, V. Vittal, and Z. Yang, "Self-healing in power systems: an approach using islanding and rate of frequency decline-based load shedding," *IEEE Trans. Power Systems*, vol. 18, pp. 174–181, 2003.

[14] D. Xu and A. A. Girgis, "Optimal load shedding strategy in power systems with distributed generation," in *IEEE PES Meeting*, 2001.

[15] I. Dobson, B. Carreras, V. Lynch, and D. Newman, "Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization," *Chaos: An Interdiscip. J. Nonlinear Science*, 2007.

[16] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, pp. 1344–1371, 2013.

[17] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vulnerability under data-centric threats," in *IEEE INFOCOM*, 2014.

[18] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, pp. 99–107, 2010.

[19] Z. Lu, W. Wang, and C. Wang, "Camouflage traffic: Minimizing message delay for smart grid applications under jamming," *IEEE Trans. Dependable and Secure Computing*, vol. 12, pp. 31–44, 2015.

[20] A. Das, J. Banerjee, and A. Sen, "Root cause analysis of failures in interdependent power-communication networks," in *IEEE MILCOM*, 2014, pp. 910–915.

[21] Y. Xu and W. Wang, "Characterizing the spread of correlated failures in large wireless networks," in *IEEE INFOCOM*, 2010.

[22] K. Srinivasan, P. Dutta, A. Tavakoli, and P. Levis, "Understanding the causes of packet delivery success and failure in dense wireless sensor networks," in *ACM SenSys*, 2006.

[23] 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.

[24] A. Bashan, Y. Berezin, S. V. Buldyrev, and S. Havlin, "The extreme vulnerability of interdependent spatially embedded networks," *Nature Physics*, vol. 9, no. 10, pp. 667–672, 2013.

[25] F. Roberts and B. Tesman, *Applied combinatorics*. CRC Press, 2009.

[26] P. P. Marino, *Optimization of Computer Networks: Modeling and Algorithms: a Hands-on Approach*. John Wiley & Sons, 2016.

[27] 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.

[28] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[29] M. J. Neely and E. Modiano, "Capacity and delay tradeoffs for ad hoc mobile networks," *IEEE Trans. Information Theory*, vol. 51, 2005.

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

[31] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International J. Electrical Power & Energy Systems*, vol. 28, pp. 627–633, 2006.