Computer Networks 158 (2019) 184–192

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Cyber and physical interactions to combat failure propagation in smart grid: Characterization, analysis and evaluation

Mingkui Wei[a,1,*], Zhuo Lu[b,1,3], Yufei Tang[c,1], Xiang Lu[d,1,2,4]

[a] Department of Computer Science, Sam Houston State University, Huntsville, TX 77341 USA
[b] Department of Electrical Engineering, University of South Florida, Tampa FL 33620 USA
[c] Department of Computer & Electrical Engineering and Computer Science, and the Institute for Sensing and Embedded Network Systems Engineering, Florida Atlantic University, Boca Raton, FL 33431 USA
[d] Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 1 February 2019
Revised 17 April 2019
Accepted 13 May 2019
Available online 17 May 2019

ABSTRACT

The smart grid is envisioned to use a cyber-physical network paradigm to prevent failures from propagating along large-scale infrastructures, which is a primary cause for massive blackouts. Despite this promising vision, how effective cyber and physical interactions are against failure 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 failure propagation by shedding a computed amount of loads based on collaborative communication. Specifically, we model failures, such as system fault, happening in the physical domain as a counting process, with each count triggering a load shedding action in the cyber domain. Although global load shedding design is considered optimal by globally coordinating shedding actions, its induced failure probability (defined as the one that at least a given number of power lines fail) is shown scalable to the delay performance and the system size. This indicates that global load shedding is less likely to stop failure propagation in large systems than local shedding 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.

1. 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 failure propagation [4–7], which is a primary cause for a number of large blackouts in history, such as the Northeast blackout of 2003 [8].

In power system, a power line has its capacity to transmit the power. If the power exceeds the capacity, the power line will become overloaded and fail. Such a failure disconnects a power line and accordingly leads to power flow redistribution across the grid, which can in turn overload other power lines, and eventually form an unstoppable failure propagation event, known as a *cascading failure* [6,7,9].

To rescue a power system from such a cascading failure, load shedding [4,10–12] 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 failure propagation. In conventional power grids, the amount and location of loads-to-shed are pre-configured and thus lacks flexibility. Assisted by the communication network, the load shedding in smart grids can be conducted in a more intelligent way [4,13]. Particularly, during a cascading failure, a control center collects global system information and uses a global optimization framework to shed the optimal amount of loads, which stops the failure propagation, and in the meanwhile keeps the load shedding cost at the minimum.

While such intelligent load shedding scheme seems promising, it does not come without compromise. The communication network that carries the control and command messages is nonetheless ideal. Packets in practical communication networks

* Corresponding author.
E-mail addresses: mwei@shsu.edu, mwei2@ncsu.edu (M. Wei), zhuolu@usf.edu (Z. Lu), tangy@fau.edu (Y. Tang), luxiang@iie.ac.cn (X. Lu).

[1] Member, IEEE

[2] A preliminary version appeared in IEEE INFOCOM 2017.

[3] supported in part by ONR N00014-16-1-2648.
[4] supported in part by NNSFC 61402476.

https://doi.org/10.1016/j.comnet.2019.05.006
1389-1286/

are subject to random delay and loss (not to mention cyber-attacks), and such incidences can easily render the intelligent load shedding ineffective, and even counter-productive, as we demonstrate in the following sections.

From a practical view on an imperfect cyber domain, cascading failures in the smart grid in fact constitutes a cyber-physical interactive process with actions affecting each other. However, there has not been any systematic study in the literature on how this interactive process works to prevent (or exacerbate) the failure propagation. In this paper, we take a combined analytic and experimental approach to model and evaluate the interactive process induced by failure propagation under load shedding, and identify the correlation between the communication performance and the effectiveness of load shedding strategies. 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 failure propagation in the smart grid.
- We find that under global load shedding, the failure probability $\mathrm{P}(M(\infty) \geq m)$ 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, our results reveal that conventional load 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 conventional and global schemes.

To the best of our knowledge, we are the first to formally characterize the cyber-physical interactions during failure 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.

The rest of the paper is organized as follows. In Section 2, we introduce the models and state our research problems. In Section 3, we present analytical results and their indications in practical design. In Section 4, we discuss the results from simulation experiments. In Section 5, we present related work. Finally, we conclude this paper in Section 6.

2. Backgrounds, models and problem statement

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

2.1. The smart grid and network architecture

In the smart grid [2,3,11], 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 (communication link) and physical (transmission line) 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. A pair of nodes are allowed to have at most one cyber edge and one physical edge.

2.2. Failure 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 [5,6,14]. When the power line fails, it is disconnected from the system. Such a disconnection in turn leads to power flow redistributed on the rest of the power lines, which, however, increases the loads on some other power lines. If the increased load on a line exceeds its capacity, the line will become fail and be disconnected from the system. This results in power redistribution and even more failures, and eventually forms a cascading failure [6–8] over the entire power grid.

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 with time t increasing, 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 probability to measure the eventual scale of failure 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 $\mathrm{P}(M(\infty) \geq m)$.

When there is no protective mechanism to stop the failure propagation, we can expect that $\mathrm{P}(M(\infty) \geq m)$ be close to 1 for a reasonably large value of m.

Remark 1. During the process of a cascading failure, an originally fully connected grid can be disintegrated into several islands, which can still maintain independent operation. Each island has independent topology, operating point, and potential cascading failures that continue to propagate therein [15]. This islanding process will eventually hinder the cascading failure process and prohibit the value m from being increased to a very large number. Therefore, when the failure stops, we only expect m to be reasonably large.

2.3. Load shedding in the cyber domain

Load shedding [4,10–12] is an effective countermeasure against cascading failures, which purposefully disconnect some load from the grid to eliminate overload on transmission lines. 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 conventional power grids works in a pre-configured manner [16]. In particular, multiple sensors, such as frequency detectors or voltage detectors, are equipped at a substation. Once the readings from such sensors reach beyond a threshold (e.g., frequency drops from 60 Hz to 59.3 Hz [17]), the power system is considered being malfunctioning, circuit breakers at preset locations will be actuated to proactively disconnect (i.e., shed) a preset amount of load with attempt to prevent failure propagation. This approach is usually not

optimal in terms of both effectiveness and cost, because such pre-configurations are solely determined by load priority (e.g., power lost at a factory may cause more economical than at a residential community), rather than how much such shed can contribute in stopping the propagation. 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 control center computes how to shed load with the minimum cost to stop failure propagation [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 dynamic global information, the algorithm guarantees the optimal solution. 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 [4,13]. However, global load shedding does depend on messaging among nodes and the control center in the cyber domain. The effectiveness of computer networking therefore becomes the key for a successful load shedding. In smart grid settings, such effectiveness is generally measured by the delay metric instead of the throughput metric [3,18]. 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.

2.4. 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 $\mathrm{P}(M(\infty) \geq m)$?
- 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.

3. Analytical formulation and results

3.1. Analyzing cyber and physical interactions during failure 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 [4–6,14,19,20] have shown that failure 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 failures exactly propagate are mathematically intractable. As 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 [19,20]. All these studies only focus on the physical domain instead of jointly considering both cyber and physical domains.

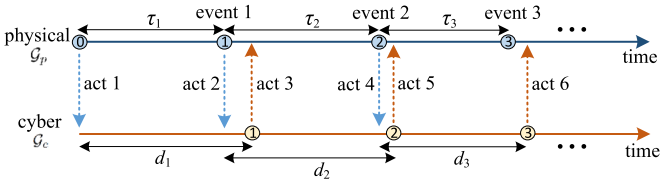


Fig. 1. Example of time events on cyber and physical domains and how they interact with each other during failure propagation under load shedding.

When communication-enabled load shedding comes into play, the failure 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 $\mathcal{G}_c$.

To offer an analytical formulation, we need to first clearly understand how the cyber and physical domains interact. Fig. 1 shows such an example from a timing perspective for modeling. Suppose in Fig. 1 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 after a time duration of τ_1 (according to Definition 1), shown as event 1 in Fig. 1. Then, the second and third failures follow, denoted as events 2 and 3, respectively, in Fig. 1. 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. 1: 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. 1) to the control center. 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. 1. 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. 1. 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. 1, it is not enough after the second failure; hence, the failure propagation continues.

3.2. Analytical results and discussions

3.2.1. Formulations and results

In Fig. 1 we demonstrate that failure 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 $\mathrm{P}(M(\infty) \geq m)$ in exact closed-form analysis.

Our strategy is to characterize $\mathrm{P}(M(\infty) \geq m)$ in a generic formulation, and adopt an asymptotic analysis approach to predict theoretically how $\mathrm{P}(M(\infty) \geq m)$ is affected by the message delivery in the cyber domain. Then, we will use system-level sim-

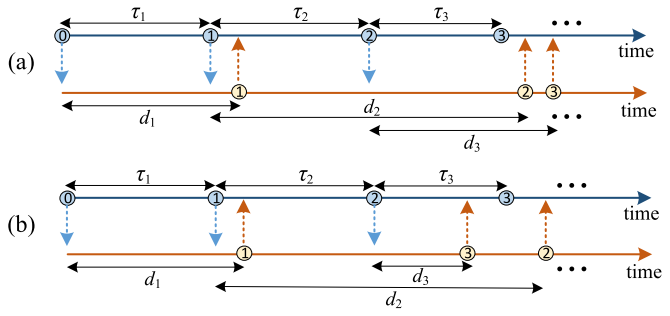


Fig. 2. Examples of how failures can keep propagating.

ulations 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 $\mathrm{P}(M(\infty)>m)$ can be derived as follows.

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

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

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* $A_{j,i}$ $(i\geq j\geq 1)$ *represents the event that the j-th load shedding is acted in the physical domain after the i-th failure happens, satisfying*

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

Proof. To obtain $\mathrm{P}(M(\infty)\geq m)$, 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 failure propagation. This can imply the case shown in Fig. 1 that each load shedding action is delayed and performed right after the next fault happens. This also includes some other cases shown in Fig. 2: (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 $A_{j,i}$ $(i\geq j\geq 1)$ 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 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 $B_2=B_1\cap\left(A_{1,2}\cup A_{2,2}\right)=A_{1,1}\cap\left(A_{1,2}\cup A_{2,2}\right)$, and $B_3=B_2\cap B_1\cap\left(A_{1,2}\cup A_{2,2}\right)=A_{1,1}\cap\left(A_{1,2}\cup A_{2,2}\right)\cap\left(A_{1,3}\cup A_{2,3}\cup A_{3,3}\right)$, and so on. By induction, we have

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

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)

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

where

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

According to the inclusion-exclusion principle [21], we can write (4) as

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

where

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

which completes the proof. □

Remark 2. 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 failure propagation speed in the physical domain $\mathcal{G}_p$.

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

Physical domain parameters $\{\tau_i\}$**:** Note that a physical failure is due to the tripping of an overloaded power line in the physical domain $\mathcal{G}_p$. The tripping process is as follows [15]: during the power redistribution, a power line starts to accumulate the heat due to overload; when the overall accumulated heat over time exceeds a pre-set threshold, the power relay will immediately trip the power line, thus removing it from the grid. This means that sooner or later, an overloaded power line will be tripped. In addition, realistic power systems may exhibit self-organized criticality (SOC) characteristics [22,23]: the cascading failure usually has a slow process with relatively large τ_i for the first few events; after passing a critical point, the cascading failure then becomes an unstoppable process with small τ_i for quick load, generation or line tripping. For our modeling and analysis, it suffices to use $\tau_i\in[\tau_{\min},\ \tau_{\max}]$ instead of assuming a particular distribution for τ_i, where $\tau_{\min}$ and $\tau_{\max}$ are constants depending on the

power system setups (e.g., overheat thresholds of power lines) and structures (e.g., size and connection).

Cyber domain parameters $\{d_i\}$**:** We assume that the action delay of load shedding $\{d_i\}$ in the cyber domain $\mathcal{G}_c$ is exponentially distributed. The exponential distribution is a widely-adopted model to facilitate analysis of link or path delay in a network [24,25]. Mathematically, the sum of exponentially distributed random variables also exhibits an exponential tail. Therefore, We assume $\{d_i\}$ following the exponential distribution.

With the two reasonable assumptions for $\{\tau_i\}$ and $\{d_i\}$, we state the next results as follows.

Theorem 2. *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 $g(\cdot)$, it holds that*

$$\log \mathsf{P}(M(\infty) > m) = -O(m)\Theta\left(\frac{1}{g(n)}\right)\Theta(f(\tau_{\min}, \tau_{\max})), \tag{8}$$

where $n = |\mathcal{N}|$ is the number of nodes in the network $\mathcal{G} = (\mathcal{N}, \mathcal{E}_c, \mathcal{E}_p)$, and $\tau_{\min} \le f(\tau_{\min}, \tau_{\max})) \le \tau_{\max}$.

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

$$\begin{aligned} \mathsf{P}(M(\infty) \ge m) &\le \mathsf{P}(A_{1,1}) = \mathsf{E}(e^{-\lambda_1 \tau_1}) \\ &\le e^{-\lambda_1 \tau_{\min}} = e^{-\Theta\left(\frac{1}{g(n)}\right)\tau_{\min}} \end{aligned} \tag{9}$$

and thus

$$\log \mathsf{P}(M(\infty) \ge m) \le -\Theta\left(\frac{1}{g(n)}\right)\tau_{\min}. \tag{10}$$

On the other hand, it holds that $\bigcap_{l=1}^{m} A_{l,l} \subset \bigcap_{l=1}^{m} \bigcup_{j=1}^{l} A_{j,l}$. Therefore,

$$\begin{aligned} \mathsf{P}(M(\infty) \ge m) &\ge \mathsf{P}\left(\bigcap_{l=1}^{m} A_{l,l}\right) = \prod_{l=1}^{m} \mathsf{P}(A_{l,l}) \\ &= \prod_{l=1}^{m} \mathsf{E}(e^{-\lambda_i \tau_i}), \end{aligned} \tag{11}$$

where λ_i is the parameter for d_i satisfying $\mathsf{E}(d_i) = 1/\lambda_i = \Theta(g(n))$, and τ_i is the interval between two subsequent physical failures.

Then, we further have,

$$\mathsf{P}(M(\infty) \ge m) \ge \prod_{l=1}^{m} \mathsf{E}(e^{-\lambda_i \tau_i}) = \prod_{l=1}^{m} \mathsf{E}\left(e^{-\frac{\tau_i}{\Theta(g(n))}}\right). \tag{12}$$

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

$$\begin{aligned} \mathsf{P}(M(\infty) \ge m) &\ge \prod_{l=1}^{m} \mathsf{E}\left(e^{-\frac{\tau_i}{\Theta(g(n))}}\right) \ge \prod_{l=1}^{m} e^{-\frac{\mathsf{E}(\tau_i)}{\Theta(g(n))}} \\ &= e^{\sum_{i=1}^{m}\left(-\frac{\mathsf{E}(\tau_i)}{\Theta(g(n))}\right)} \ge e^{-m\Theta\left(\frac{1}{g(n)}\right)\tau_{\max}}, \end{aligned} \tag{13}$$

where the last inequality holds because $\tau_i \le \tau_{\max}$ and then $\mathsf{E}(\tau_i) \le \tau_{\max}$. We further have

$$\log \mathsf{P}(M(\infty) \ge m) \ge -m\Theta\left(\frac{1}{g(n)}\right)\tau_{\max}. \tag{14}$$

Combining (10) and (14) finishes the proof. □

3.2.2. Discussions and observations

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.

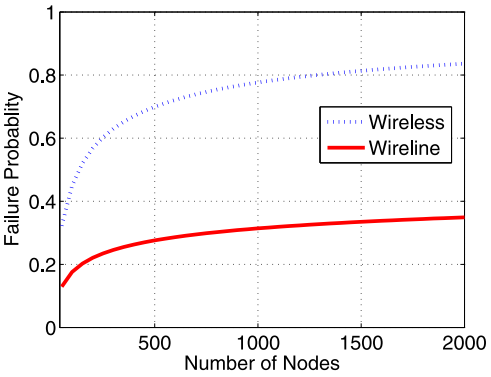


Fig. 3. Examples: the failure probabilities given a fixed $m = 100$ under global load shedding in wireless and wireline based cyber domains with average delays on the order of $\Theta(\sqrt{n})$ and $\Theta(\log(n))$, respectively.

Impact of Network Architecture on Global Shedding: 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 [26]), 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 $\Theta(\sqrt{n})$ [27], thereby $g(n) = \Theta(\sqrt{n})$.

Fig. 3 shows a numerical example to compare 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. 3 that the 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 [3,25], it is still less suitable for failure prevention than wireline networking in large-scale systems.

Impact of Network Architecture on Local Shedding: For local load shedding design, it only requires shedding a preset amount of loads in local deployments within limited scopes. Suppose that local shedding makes decisions among $l(n) \le n$ nodes. Then, it only incurs a delay of $g(n) = \Theta(\log l(n))$ for wireline or $g(n) = \Theta(\sqrt{l(n)})$ for wireless. In particular, when $l(n) = \Theta(1)$, we obtain $g(n) = \Theta(1)$ for both wireline and wireless, which leads to the failure probability in (8) not scaling with n. Comparing this bound with those due to global load shedding illustrated in Fig. 3, we conclude that interestingly, global shedding cannot be viewed as a uniformly better solution than local shedding when n is large, because the failure probability due to global shedding scales with n.

Use of Wireless Networking to Stop Cascading Failure: If wireless networking is indeed to be deployed in a smart grid system, we note that local shedding within a constant scope would be a better solution to prevent a cascading failure from happening. In addition, we should always avoid deploying a purely wireless architecture for communication because global shedding over multi-hop wireless networking can be very risky. Hence, using wireless only as the last mile delivery would be a better solution when global shedding is used.

Next, we move on to system-level simulations to validate theoretical predictions and characterize failure propagation process under load shedding with practical settings.

4. System-level simulations

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

4.1. System configurations

4.1.1. Physical domain

We use two power systems for the simulation [28]: the IEEE 57-bus system that contains 57 buses, 80 transmission lines, with total generation 1250 megawatts (MW); and the IEEE 118-bus system that contains contains 118 buses, 186 transmission lines, and 19 generators, with a total load of 3,668(MW). 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 (AC model is not ususally used for cascading failure modeling in literature due to its complexity [29–31]).

4.1.2. Cyber domain

We model the communication network and the power grid to have a 1-to-1 mapping, i.e., each bus in the power grid is associated with 1 communication node. It has been shown in related study [24,32] that the distribution of packet delay in a generalized network follows the exponential distribution. And thus we do not make assumption of any particular topology of the communication network, rather, for each message generated during a cascading failure, we associate it with a random delay that follows the same exponential distribution, with its parameter adjustable during the simulation.

4.1.3. Process of failure propagation under load shedding

The capacity of each power line is set to be 1.1 times higher than the normal power flow value. The simulation randomly chooses one transmission line and removes it from the system to triger the cascading failure[5] Whenever a power line fails, the nodes at both ends can detect this failure and send messages to the control center. Based on the information, the control center will calculate for a load shedding decision [4,13] and inform the nodes to act accordingly. This process continues until either there is no overload in the system, or all lines that connecting generators have been disconnected.

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

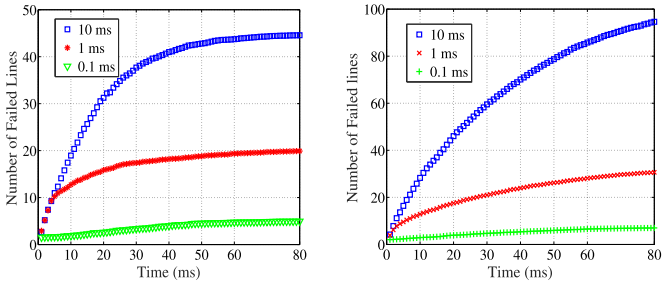
4.2. Simulations and results

The simulations were conducted based on Matlab, where we composed the code according to classical DC power flow models [33].

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

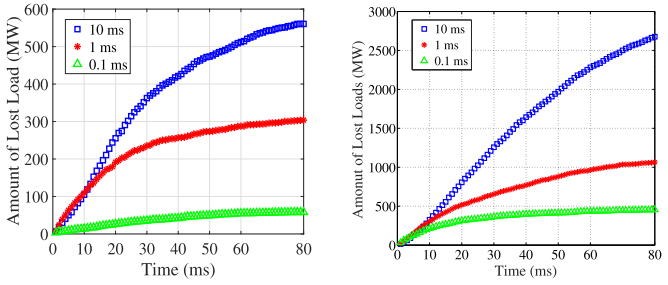
- Global load shedding with practical link performance: this is to measure how practical communication link performance in the cyber domain can affect the results of failure propagation under global load shedding.

[5] Practical power grid has N-1 tolerance. Since our purpose is to learn the character of cascading failures, this restriction does not apply to our study, i.e., for a N-1 system, we simply simulate 2-line failure as the trigger failure and it does not affect how cascading failure propagates.



(a) 57-bus (b) 118-bus

Fig. 4. The average number of failed lines over time with failure propagation under global load shedding. The average link delay is set to be 0.1 ms, 1 ms, or 10 ms.



(a) 57-bus (b) 118-bus

Fig. 5. The average amount of lost loads over time with failure propagation under global load shedding. The average link delay is set to be 0.1 ms, 1 ms, or 10 ms.

- 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.

4.2.1. Global load shedding with practical link performance

In Fig. 4 we demonstrate the average numbers of failed lines over time with failure propagation under global load shedding. The average link delay varies from 0.1 ms to 10 ms; and Fig. 5 shows the average amounts of lost loads due to line failure associated with the same simulations in Fig. 4.

Observing Figs. 4 and 5, we find the results for 57-bus and 118-bus systems are very similar. Therefore, in the following we will discuss based on the result from the 57-bus system. From Figs. 4(a) and 5(a), we can see 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, 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.

Figs. 4 and 5 also show that when the average link delay changes 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. 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. 4 and 5 show that a better cyber domain enables global load shedding to be an effective way. On the other

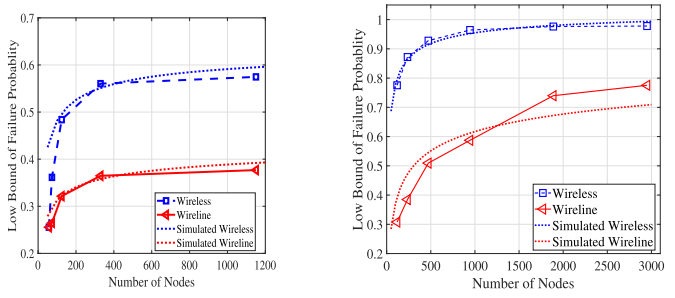


Fig. 6. The failure probability under global load shedding in wireless and wireline networks.

hand, however, 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. Therefore, we should always consider the random cyber domain factors in smart grid system design.

4.2.2. Global load shedding in wireline and wireless networks

According to our prediction in Fig. 3, 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.

Fig. 6 measures the failure probability $\mathrm{P}(M(\infty) \geq m)$ with (a) $m = 32$ for 57-bus system and (b) $m = 74$ for 118-bus system, respectively (indicating that at least 40% of the lines in the physical domain fail) as a function of the number of nodes n. We observe that Fig. 6 exhibits similar trend to the theoretical predictions of the lower bounds in Fig. 3. 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.

4.2.3. 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.

Figs. 7(a) and 7(b) show the average numbers of failed lines in the 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 Figs. 7(a) and 7(b) 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 shedding should only be considered optimal when the cyber domain sufficiently supports its actions. The same conclusion can be made from Figs. 7(c) and 7(d).

4.3. Discussions and future works

4.3.1. Hybrid local-global 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 failure and also finds high delay in message delivery, it should act immediately to shed a preset amount of loads.

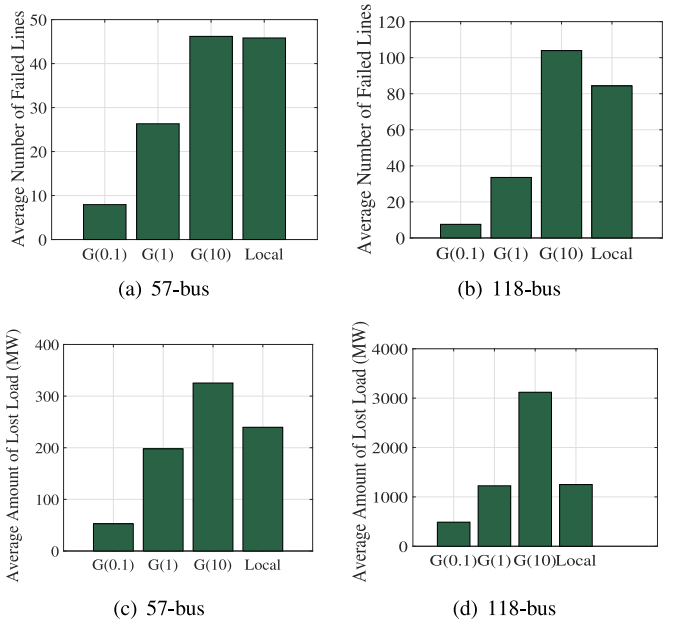


Fig. 7. The average amounts of failed line and lost loads under global and local load shedding schemes. G(0.1), G(1), and G(10) denote global load shedding with average link delay of 0.1 ms, 1 ms, and 10 ms, respectively.

4.3.2. 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 cyber-physical design involving both cyber and physical domains.

4.3.3. Fidelity and capability

Admittedly, the power system is a very complex system, therefore, similar to most existing studies, the system model proposed in this paper is only capable to reflect the smart grid behavior from a certain perspective. Nevertheless, we argue the merits of the model lie in the following aspects. First, we mathematically modeled the behavior of failure propagation in smart grids, and proposed to use τ_i, the delay in the physical domain, and d_i, the delay in the cyber domain, to characterize such failure propagation. We purposefully generalize the definition of these two parameters, and do not impose a specific topology/technology on them, such that the model can be easily migrated to evaluate the performance smart grid systems, even with more realistic setup and larger scale. Second, the conclusion made by this study, although is "as-expected" (i.e., worse communication performance incurs worse failure propagation), provides numerical result to show "how bad" the result can be under a certain configuration of the communication network. To this end, our work is able to assist not only qualitative, but also quantitative, design and planning of smart grids. And we regard the elaboration of the system model to incorporate more power system details as one direction of our future works.

5. Related works

5.1. The use of wireless technologies in the power system industry

As a matter of fact, the wireless is not a completely new technology to power systems, and has been used for decades for system monitoring, data gathering and meter reading [34].

For instance, Smart Meters transmit meter readings to a local aggregater using wireless band on 902 MHz. However, in the new era of the Smart Grid, a more reliable, secure and well-designed communication network is in high demand to accommodate more advanced power system operations, such as substation protection. In [35,36], the authors compared various wireless technologies, including WiFi, WiMax, and Cellular, etc, evaluated their performance and proposed proper use cases. The adoption of wireless technologies has also been considered and evaluated by National Institution of Standards and Technology (NIST), and an Action Plan has been published as a guideline [34]. Notwithstanding, as has also been pointed in the Action Plan [34], since the power system is such a critical infrastructure that can not afford any disruption, the power system migration from wired to wireless is a largely a local administrative decision, and the adoption of a specific wireless technology mainly depends on the manufacture. For example, Schneider Electric provides short-range wireless substation solution based on ZigBee PRO Green Power (ZGP) [37], and General Electric (GE) offer multiple solutions including licensed/unlicensed wireless band, as well as cellular [38]. The work we demonstrated in this paper does not make any assumption on specific wireless technologies. Rather, we generalize the communication network into a generalized network, and use the cyber domain delay d_i to characterize its performance, which can be easily adjusted to fit a specific technology or setup.

5.2. Related studies in failure propagation

There are generally three approaches to characterize the impacts of failure propagation in the literature.

- Analytical modeling: this line of the work is the earliest approach toward studying and understanding the cascading failure in power grids, which is generally based on a highly abstract complex or interdependent network model in relatively scientific settings (e.g., [6,19,20]), where a line failure is usually associated with a constant probability. The main objective is to analyze the eventual connectivity due to failures in a generalized complex network, e.g., the power grid. Because of this reason, many researches in this approach do not necessarily consider special characters of how power flows through power transmission lines, and use generic metrics such as node degree or centrality [6,20]. Compared to this line of research, our work focus on understanding the cascading failure specifically in the power grid by applying the Direct Current (DC) power flow model in out simulation.
- Event or simulation based analysis approach: this approach has been widely adopted with a more practical view on realistic power engineering settings (e.g., [9,10,13]). Existing studies either analyze the historic events to understand how failures propagate, or use power system cascading failure model, such as the OPA model [39] and interaction model [40], to simulate and evaluate the failure propagation. In most studies from this line or research, the underlying communication network is implicitly assumed to be perfect.
  For instance, in the OPA model [39] and other more advanced models developed by *I.Dobson*, et al., the condition of communication is not mentioned, but it is assumed that the load shedding decision is always know immediately at each bus, which indicates an ideal communication network.
  Further, in the literature [4,12,13,16], 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. Compare to this line of research, our work proposes a more realistic model that considers the impact of practical communication network with anomalies.
- Hybrid techniques considering interdependence: some studies (e.g., [5,14,41–43]) analyze the interdependence between the cyber and physical domains in smart grid from a connectivity perspective. The shortage of this line of research lies in that they focus on understanding how does the interdependency exacerbate the failure propagation, but neglect that such interdependency could have been helpful. Our work explores this under-studied area and tries to identify the transition of such interdependency from being helpful to being harmful.

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 failure propagation.

6. Conclusions

In this paper, we provided a systematic study via analytical modeling and system-level simulations on characterizing cyber-physical interactions during failure 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 design and a joint view on cyber-physical domains for any design in the smart grid.

Conflict of interests

Wei, Mingkui
Sagduyu, Yalin
Lu, Xiang
Zhuo, Lu
Tang, Yufei
Li, Jason
Ding, Lei
Wenye, Wang
Jie, Wang
Xuexue, Han
Xiaoyan, Zhu
He, Haibo
DiPippo, Lisa
Sun, Yan
Vaccaro, RIchard
August, Peter

References

[1] H. Farhangi, The path of the smart grid, IEEE Power Energy Mag. 8 (2010) 18–28.
[2] X. Fang, S. Misra, G. Xue, D. Yang, Smart grid - the new and improved power grid: a survey, IEEE Commun. Surv. Tutor. 14 (2012) 944–980.
[3] W. Wang, Y. Xu, M. Khanna, A survey on the communication architectures in smart grid, Comput. Netw. 55 (2011).
[4] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, G. Zussman, Power grid vulnerability to geographically correlated failures - analysis and control implications, IEEE INFOCOM, 2014.
[5] O. Yagan, D. Qian, J. Zhang, D. Cochran, Optimal allocation of interconnecting links in cyber-physical systems: interdependence, cascading failures, and robustness, IEEE Trans. Parallel Distrib. Syst. 23 (2012) 1708–1720.
[6] H. Xiao, E.M. Yeh, Cascading link failure in the power grid: apercolation-based analysis, IEEE ICC, 2011.
[7] J. Yan, Y. Zhu, H. He, Y. Sun, Multi-contingency cascading analysis of smart grid based on self-organizing map, IEEE Trans. Inf. Forens. Secur. 8 (2013) 646–656.

[8] J. Minkel, The 2003 northeast blackout - five years later, Sci. Am. 13 (2008).
[9] J.-W. Wang, L.-L. Rong, Cascade-based attack vulnerability on the US power grid, Safety Science 47 (2009) 1332–1336.
[10] P. Pourbeik, P.S. Kundur, C.W. Taylor, The anatomy of a power grid blackout, IEEE Power Energy Mag. 4 (2006).
[11] M. Sechilariu, B. Wang, F. Locment, Building integrated photovoltaic system with energy storage and smart grid communication, IEEE Trans. Indus. Electron. 60 (2013) 1607–1618.
[12] H. You, V. Vittal, Z. Yang, Self-healing in power systems: an approach using islanding and rate of frequency decline-based load shedding, IEEE Trans. Power Syst. 18 (2003) 174–181.
[13] I. Dobson, B. Carreras, V. Lynch, D. Newman, Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization, Chaos 17 (2007).
[14] A. Das, J. Banerjee, A. Sen, Root cause analysis of failures in interdependent power-communication networks, in: IEEE MILCOM, 2014, pp. 910–915.
[15] J. Yan, Y. Tang, H. He, Y. Sun, Cascading failure analysis with DC power flow model and transient stability analysis, IEEE Trans. Power Syst. 30 (1) (2015) 285–297.
[16] D. Xu, A.A. Girgis, Optimal load shedding strategy in power systems with distributed generation, IEEE PES Winter Meeting, 2001.
[17] Underfrequency Load Shedding2006Assessment and Review [Online]. Available: http://www.ercot.com.
[18] W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges, Comput. Netw. 57 (2013) 1344–1371.
[19] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (7291) (2010) 1025–1028.
[20] A. Bashan, Y. Berezin, S.V. Buldyrev, S. Havlin, The extreme vulnerability of interdependent spatially embedded networks, Nature Phys. 9 (10) (2013) 667–672.
[21] F. Roberts, B. Tesman, Applied Combinatorics, CRC Press, 2009.
[22] S. Mei, F. He, X. Zhang, S. Wu, G. Wang, An improved opa model and blackout risk assessment, IEEE Trans. Power Syst. 24 (2) (2009) 814–823, doi:10.1109/TPWRS.2009.2016521.
[23] S. Mei, X. Zhang, M. Cao, Power Grid Complexity, Springer Science & Business Media, 2011.
[24] P.P. Marino, Optimization of Computer Networks: Modeling and Algorithms: a Hands-on Approach, John Wiley & Sons, 2016.
[25] Y. Wang, M.C. Vuran, S. Goddard, Cross-layer analysis of the end-to-end delay distribution in wireless sensor networks, IEEE/ACM Trans. Netw. 20 (2012) 305–318.
[26] D.J. Watts, S.H. Strogatz, Collective dynamics of small-world networks, Nature 393 (6684) (1998) 440–442.
[27] M.J. Neely, E. Modiano, Capacity and delay tradeoffs for ad hoc mobile networks, IEEE Trans. Inf. Theory 51 (2005).
[28] Power Systems Test Case Archive, [Online]. Available: https://blog.schneider-electric.com/electricitycompanies/2016/05/17/distribution-substation-goes-wireless/.
[29] P. Crucitti, V. Latora, M. Marchiori, A topological analysis of the italian electric power grid, Phys. A 338 (1) (2004) 92–97.
[30] D.P. Nedic, I. Dobson, D.S. Kirschen, B.A. Carreras, V.E. Lynch, Criticality in a cascading failure blackout model, Int. J. Electr. Power Energy Syst. 28 (2006) 627–633.
[31] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, S. Mei, A multi-timescale quasi-dynamic model for simulation of cascading outages, IEEE Trans. Power Syst. 31 (4) (2016) 3189–3201, doi:10.1109/TPWRS.2015.2466116.
[32] J.-C. Bolot, Characterizing end-to-end packet delay and loss in the internet, J. High Speed Netw. 2 (3) (1993) 305–323.
[33] J.J. Grainger, W.D. Stevenson, W.D. Stevenson, et al., 2003.
[34] N.P.A. Plan, 2-guidelines for assessing wireless standards for smart grid applications, Natl. Inst. Stand. Technol. Std. (2011).
[35] P.P. Parikh, M.G. Kanabar, T.S. Sidhu, Opportunities and challenges of wireless communication technologies for smart grid applications, in: IEEE PES General Meeting, IEEE, 2010, pp. 1–7.
[36] P.P. Parikh, T.S. Sidhu, A. Shami, A comprehensive investigation of wireless lan for iec 61850–based smart distribution substation applications, IEEE Trans. Ind. Inf. 9 (3) (2013) 1466–1476.
[37] The Distribution Substation Goes Wireless[Online]. Available: https://www.gegridsolutions.com/Communications/Wireless.htm.
[38] Industrial Wireless, [Online]. Available: https://www.ee.washington.edu/research/pstca/.
[39] H. Ren, I. Dobson, B.A. Carreras, Long-term effect of the n-1 criterion on cascading line outages in an evolving power transmission grid, IEEE Trans.Power Syst. 23 (3) (2008) 1217–1225.
[40] J. Qi, K. Sun, S. Mei, An interaction model for simulation and mitigation of cascading failures, IEEE Trans. Power Syst. 30 (2) (2015) 804–819.
[41] M. Parandehgheibi, E. Modiano, Robustness of interdependent networks: the case of communication networks and the power grid, IEEE GLOBECOM, 2013.
[42] Z. Huang, C. Wang, M. Stojmenovic, A. Nayak, Characterization of cascading failures in interdependent cyber-physical systems, IEEE Trans. Comput. 64 (8) (2015) 2158–2168, doi:10.1109/TC.2014.2360537.
[43] M. Rahnamay-Naeini, M.M. Hayat, Cascading failures in interdependent infrastructures: an interdependent markov-chain approach, IEEE Trans. Smart Grid 7 (4) (2016) 1997–2006.

Mingkui Wei is an Assistant Professor in the Department of Computer Science at Sam Houston State University. He graduated as a PhD student from the Department of Electrical and Computer Engineering of North Carolina State University in 2016. And he has been working at Bell Labs prior to joining NCSU. His current research interests are in digital forensics, including computer, mobile and network forensics; and in cyber-physical system security analysis and evaluation, which covers Smart Grid and Intelligent Transportation Systems.

Dr. Zhuo Lu is an Assistant Professor in Department of Electrical Engineering, University of South Florida. He is also affiliated with the Florida Center for Cybersecurity and by courtesy with Department of Computer Science and Engineering. He currently leads the Communications, Security, and Analytics (CSA) Lab at University of South Florida. His research has been supported by NSF, ARO, ONR, DOE and Florida Center for Cybersecurity. Dr. Lu received his Ph.D. degree from North Carolina State University in 2013. Dr. Lu's research has been mainly focused on modeling and analytical perspectives on communication, network, and security. His recent research is equally focused on practical and system perspectives on networking and security. He is a member of ACM and IEEE.

Yufei Tang is an Assistant Professor in the Department of CEECS and a Faculty Fellow of I-SENSE at Florida Atlantic University (FAU), where he is also the director of the Intelligent and Resilient Systems (IRS) Research Group. He received his Ph.D. in Electrical Engineering from the University of Rhode Island (URI) in 2016. His research includes Computational Intelligence (e.g., Machine Learning, Networked Data Mining) and Cyber-Physical Systems (e.g., IoT, Smart Grid, Critical Infrastructure Systems).

Xiang Lu obtained his Ph.D. degree from Department of Computer Science at Xidian University, with Dr. Jianfeng Ma and Dr. Wenye Wang. From 2009 to 2012, he was a visiting Ph.D. student at the Department of Electrical and Computer Engineering, North Carolina State University. In NCSU, he worked in the FREEDM system center as a research assistant to design communication systems for power electronic devices. In Spring 2013, he joined the Institute of Information Engineering, CAS, as an assistant professor.His current research is related to computer and network security, with an emphasis on performance and vulnerability analysis of security schemes in practical applications and systems. He is also working on cyber-physical system security, especially in those emerging areas, like the smart grid, video surveillance systems, and so on.