Combat the Disaster: Communications in Smart Grid Alleviate Cascading Failures

Mingkui Wei
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC, 27606
Telephone: 919-513-7260
Email: mwei2@ncsu.edu

Wenye Wang
Department of Electrical and Computer Engineering
North Carolina State University
Raleigh, NC, 27606
Telephone: 919-513-2549
Email: wwang@ncsu.edu

Abstract—**Cascading failure is one of the most catastrophic events in power grid, which refers to large scale power system outage caused by the rampant spread of small scale system fault or even single device failure. Its disastrous result is expected to be mitigated in the scope of smart gird, in which communication enabled smart devices exchange critical information to preclude such events. To carry the concept into reality, one pivotal step is quantitative study of the benefit smart grid can bring, i.e.,** ***to what extent smart grid can improve power system stability, specifically, in combating cascading failure?*** **We identify three aspects,** ***time*****,** ***space*****, and** ***scale*****, which are needed for thorough evaluation of the impact of a cascading failure, and further propose a new cascading failure model which is able to depict all three aspects with numerical results. Our observations explicitly suggest that communication between power devices is essential in alleviating the impact of cascading failure, and that even a basic information exchange among limited number of power devices could significantly ameliorate the aftermath of a cascading failure in power grid.**

I. Introduction

Cascading failure (also known as *blackout*) in power grid is notoriously known as one of the most devastating force, which usually results in disastrous result to modern societies. As its name indicates, cascading failure is a domino-like large scale system failure, which is initially triggered by incorrectly or untimely handled small scale or even single device failure.

On the other hand, as the promising successor of the aged traditional power grid, smart grid is expected to mitigate such disastrous events, and bring a more stable and reliable power system. This expectation stems from the underlying communication network of smart grid: with most power devices being granted the capability to communicate with their peers, essential information such as system operating status and fault events can be shared within the power system, which facilitates a more prompt reaction on unexpected contingencies.

To bring the concept of smart grid to reality and use it to leverage the traditional power grid, it is imperative to quantitatively evaluate the benefit that smart grid can bring, i.e., to gain numerical results on the improvement smart grid contributes regarding system stability, because only when we have accurate evaluation results, can we efficiently and effectively allocate our limited research resources and efforts.

In this paper, we study a more specific question and explore that *how and to what extent can smart grid help in alleviating the aftermath of cascading failures*? The answer to this question is extremely important in smart grid study, not only because smart grid is expected to combat this disastrous event, but also because new threats – cyber attacks stem from its underlying communication networks – might be introduced and even exacerbate the situation instead [1], [2].

Two elements are necessary to solve this question. First, a set of proper metrics/criterion which numerically and precisely depict the impact of a cascading failure, and second, a cascading failure model which is able to reflect those metrics/criterion.

To tackle the first problem, we identify 3 aspects to thoroughly evaluate the impact of a cascading failure, which are: *time*, when does a failure happen, how long it lasts, and how fast it propagates? *Space*, how far can a cascading failure reach? And *scale*, how many components are impacted?

Regarding the second problem, we find traditional cascading failure models are insufficient to reflect the dynamic features from all three aspects, and this fact motivates us to propose a new model regarding cascading failure. We denote two features which distinguish the new model from generic ones.

1) Our model is built in real-time power systems simulator. Most existing cascading failure models [3]–[5] use graph to represent power system, in which power devices and transmission lines are mapped into nodes and edges. Electrical properties such as resistance on transmission lines, or the speed of electricity flow, are neglected as they will make those models over complicated. However, this simplification makes those models unable to reflect the *time* and *space* aspects. We solve this problem by building our cascading failure model in PSCAD [6], a real time power systems simulator, which accurately models power devices, and therefore is able to depict system status in transient time.

2) We consider *overcurrent* is the root cause of a cascading failure. Most existing cascading failure models make the assumption that *overload* is the sole cause of the failure, which is a reasonable but not accurate simplification [7], [8]. In reality, the cause of cascading failure is more complex, and fault current, which can be caused by overload but also

possible by other events such as a ground-transmission line short circuit (e.g., a tree touches a transmission line), plays a significant role in the initiation and propagation of a cascading failure [8]. The overcurrent assumption covers more causes regarding a cascading failure and therefore more practical.

In order to evaluate the benefit of smart grid in alleviating the consequence of cascading failure, we assume that adjacent devices are able to communicate and inform each other of a fault, and run the simulation based on our new model. Our simulation endorses the advantage of smart grid by showing that even a basic information exchange between limited number of power devices could significantly reduce the impact of a cascading failure.

Our contribution can be summarized as follows:

1) We build a new cascading failure model in real time power system simulator, which enables us to evaluate the impact of a cascading failure from various aspects.

2) We assume the cascading failure is caused by *overcurrent*, rather than *overload*, which is used as the root cause of cascading failure in existing cascading failure models. Overcurrent can be caused by various events, such as short circuit, lighting, or overload, and is more consistent with real world cases.

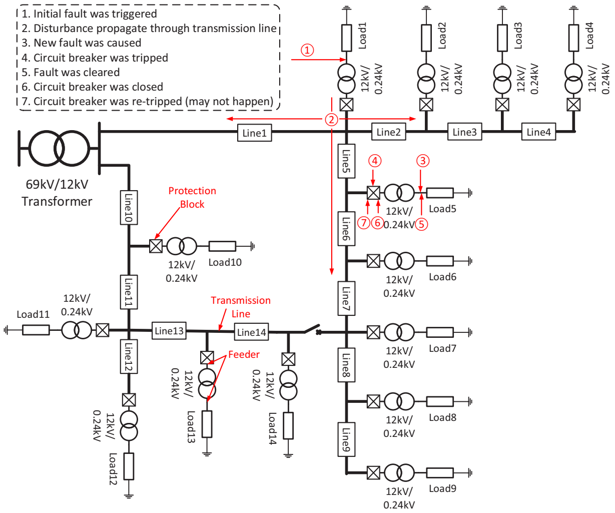
3) Our numerical results endorse the benefits brought by smart grid, and show that even a basic information exchange among limited number of power devices can significantly alleviate the aftermath of a cascading failure.

The organization of this paper is as follows. In Section II we introduce related works and background of our model. In Section III we demonstrate the cascading failure model. In Section IV we present and discuss simulation results, and in Section V we conclude our work.

II. Background

There are a lot of works on modeling cascading failure [4], [9]–[14], and most of them share the same basis, that they assume the overload as the sole root cause of any failure. Particularly, in those models, a node-edge topological graph is formulated, while the node represents either load consumer or generator, and the edge represents power transmission line. It is assumed that nodes consume/generate load and edges carry load to other nodes, and both nodes and edges have fixed capacity, beyond which they fail and will be removed. The cascading failure begins by removing a node/edge from the graph. The removal causes load redistribution on remaining edges and nodes, and potentially more nodes/edges overload.

The overload assumption is favored by researchers because its flexibility and ease to be applied, i.e., it can be easily modified to adapt various assumptions. For instance, in a complex network theory based cascading failure model [3], the electrical properties can be totally neglected and the “load” can be simply substituted with the node degree, or “betweenness” [9]. Even in advanced models in which electrical properties are considered, such as the Direct Current (DC) or Alternating Current (AC) models [12], [13], load is much easier to be calculated than other electrical parameters such as voltage or current. However, the overload assumption suffers as it is unable to reflect temporal and spacial features. In overload based cascading failure models, edges are usually unweighted and undirected, thus if a node fails, all its neighbors will be equally affected simultaneously, which is not true in practice.



(a) Single line diagram of model prototype

```
for each_load

  if (Current > C_t) && (trip_counter == 0)
    if (overcurrent_last_time > T_flt)
      TRIGGER SelfFault;
    end if
    if SelfFault_last_time > T_brk
      TRIP circuit breaker;
    end if
    if trip_last_time > T_clr
      CLEAR fault;
    end if
    if fault_clear_last_time > T_rc
      RECLOSE circuit breaker;
    end if
  end if

  if (Current > C_t) && (trip_counter == 1)
    if(overcurrent_last_time > T_rc)
      TRIP circuit breaker permanently;
    end if
  end if

end
```

(b) Operation of protection block

Fig. 1. Physical power system prototype

As a matter of fact, as pointed in [7], [8], large scale blackouts are usually caused by large current disturbance (such as a short circuit current caused by the contact among tree branches and transmission lines, as shown a significant factor during 2003 southeast America blackout [15]), where overload just serve as a special case which can cause such disturbance.

III. Modeling of Cascading Failure

Shown in Fig. 1(a) is a 14 bus power system that is used in our study, which is abstracted from power system in a city nowadays and we name it as the Green Hub. A key component is the “protection block” we built in our model, whose operation is shown in Fig. 1(b). The protection block is a mimic of a real relay, which picks up current value, compares with overcurrent threshold, trips the circuit breaker

TABLE I
PARAMETERS

Notation	Description
$C_t(i)$	Overcurrent threshold, current exceeds this threshold is regarded as overcurrent.
$T_{flt}(i)$	Fault time. The time a feeder can tolerant the overcurrent. Beyond this time a fault will be caused on a feeder.
$T_{brk}(i)$	Break time. If a fault exists on a feeder longer than this time, the relay will trip the circuit breaker and disconnect the load from power grid.
$T_{clr}(i)$	Fault clear time. After a load (feeder) is disconnected from power grid after this time, the fault will be cleared.
$T_{rc}(i)$	Reclose time. When the fault is cleared after this time, the circuit breaker will be reclosed and the load will be reconnected to power grid.
$T_{rt}(i)$	Re-trip time. If current still larger than C_t after being reconnected, circuit breaker will trip *permanently* again if overcurrent exists longer than this time.

note: $i \in [1, N]$, where $N = 14$ in our model. For simplicity we assume all 14 loads have the same value, and omit 'i' in the following discussion.

when overcurrent happens, and reconnects the load back to main power grid when fault is cleared.

We assume the cascading failure is initialized by a current disturbance caused by a short circuit fault happened on a feeder. The current disturbance, which is multiple times of the value in normal operation, propagates along the power transmission line to all other loads. Each feeder has a threshold current, C_t. At the loads whose current exceeds C_t, the feeder dose not fail immediately, instead, the feeder is able to tolerant the overcurrent for a period of time, which is denoted by T_{flt}. If the overcurrent exists longer than T_{flt}, the feeder will fail and fall into fault(e.g., overcurrent causes overheat, and the overheat causes the feeder sag and touch other feeder/tree branch), which propagates to even more devices.

In practice, most faults are non-persistent [16] and could be self-cleared if the faulted feeder is disconnected from the power grid in time (e.g., before it melt down). And we use T_{brk} to model the time period from the time when fault happens on a feeder, to the time when the circuit breaker is tripped. The fault on the feeder will take T_{clr} to be self-cleared after being disconnected, and after T_{rc}, the circuit breaker will reclose and the feeder will be connected back to power grid.

However, it is possible that when the feeder is re-connected to the power grid, the current is still larger than its threshold C_t. If this condition exists for another time period T_{rt}, the circuit breaker will permanently trip and the load will be left disconnected until the end of simulation.

In order to demonstrate how does a cascading failure initiate and propagate in a much clearer way, we take a snapshot of the current of a load and denote each time point and time interval, and show it in Fig. 2.

IV. Simulation Setup and Results

In table II we list all the parameter values we used in our simulation. Those values are chosen to be within reasonable range according to industry standard [16], as well as facilitate

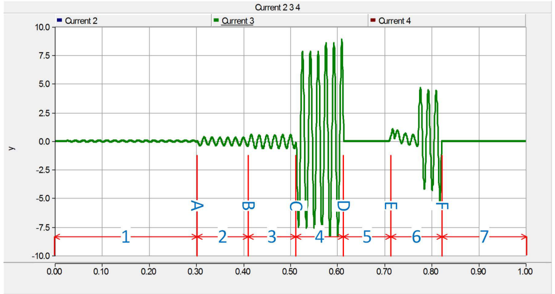


Fig. 2. An example of cascading failure scheme. Time-points: A. Current rise because fault is caused at other loads, but current is below C_t; B. As fault propagate, fault current rise beyond C_t; C. Self-fault is caused; D. Circuit breaker tripped; E. Re-connected, but fault still exists; F. Re-tripped. Time-intervals: 1. Unspecified; 2. Unspecified; 3. T_{flt}; 4. T_{brk}; 5. T_{rc} + T_{clr}; 6. T_{rt}; 7. Unspecified

TABLE II
INITIAL VALUE OF PARAMETERS

Par	Value	Range during simulation
C_t	250 A	na
T_{flt}	0.1 sec	0.05sec - 0.2sec, with 0.01sec step
T_{brk}	0.1 sec	0.03sec - 0.10sec, with 0.01sec step
T_{clr}	0.05 sec	na
T_{rc}	0.1 sec	na
T_{rt}	0.1 sec	na

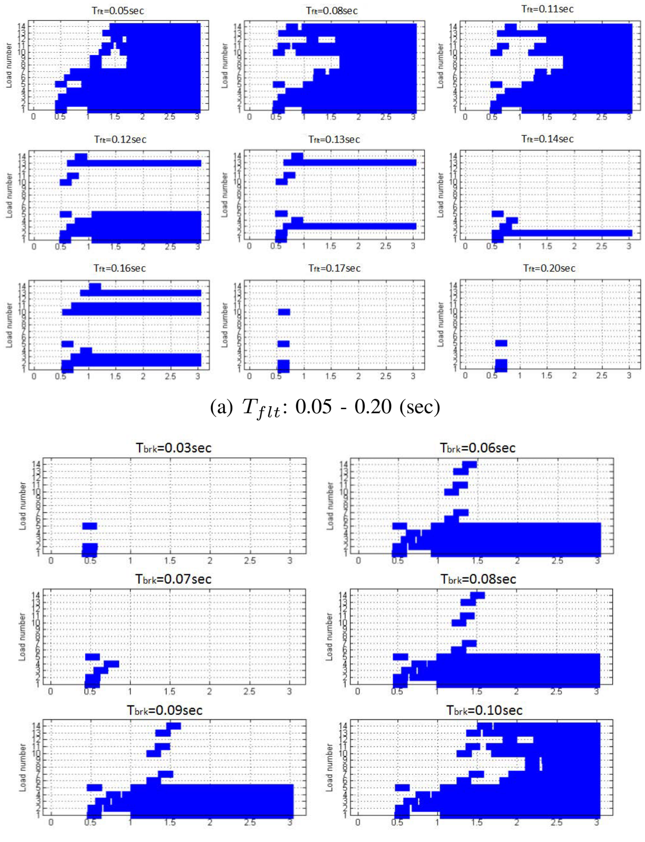
the presentation of our simulation result. In our simulation we vary the value of each parameter and observe the results. Due to the page limit, in this paper we show the results of two parameters, T_{flt} and T_{brk}, which typically represent our observation. Without loss of generality, in following simulation we always assume the initial failure happens at load 1.

A. Result evaluation

As shown in Fig. 3 and Fig. 4, we use 2 figures to reveal the *time*, *space*, and *scale* of a cascading failure.

1) Parameter snapshot: We draw a series of 2-dimensional figures to show the impact caused by the change of a particular parameter. For each figure, the x-axis represents simulated time, and y-axis is the index vector for 14 buses. During the process of one simulation, if a feeder becomes fault, we mark on the figure according to the fault time period. For instance, if feeder 1 experiences fault during the time from 1 second to 2 seconds, the line with ($y = 1$, $1 \leq x \leq 2$) will be marked as blue in the figure. The set of snapshot figures can not only show how does a parameter impacts the result of a cascading failure, but also indicate most susceptible loads.

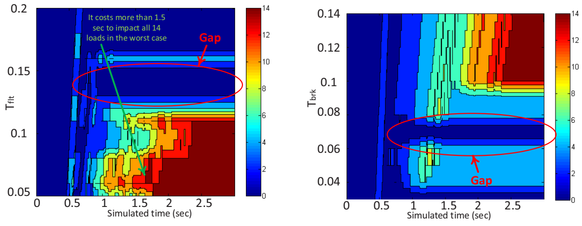
2) Parameter contour: We synthesis the set of snapshot figures and draw a 3-dimensional contour, in which the x-axis is still the simulated time, but we let y-axis represent the variation of the simulated parameter. And we use different color to indicate the severity of a cascading failure, i.e., how many loads are under fault. For example, as shown in Fig. 4, a color that approximate to red means more loads are experiencing fault, while a color close to blue means the reverse. Compared with the snapshot figure, the contour



(a) T_{flt}: 0.05 - 0.20 (sec)

(b) T_{brk}: 0.03 - 0.10 (sec)

Fig. 3. Parameter snapshot for varying T_{flt} and T_{brk}.



(a) T_{flt}: 0.05 - 0.20 (sec)

(b) T_{brk}: 0.03 - 0.12 (sec)

Fig. 4. Parameter contour for varying T_{flt} and T_{brk}.

focuses more on illustrating the consequence of a cascading failure in system level, as it only reflects how many loads are under fault without specify their indices.

B. Observation and discussion

1) It explicitly shows that a minute calibration in parameter can result in significant system state change. For each parameter, every 10 milliseconds change in its value causes the system to react very differently. For some critical steps, such as from $time = 0.09seocnds$ to $time = 0.10seconds$ in Fig. 3(b), a 10 milliseconds change makes the number of finally tripped loads jump from 5 to 14. These results signify the importance of policy-making and parameter-setting in fault management of power system: with a sound protection policy in which all parameters are carefully calibrated and validated, the risk of a cascading failure can be significantly reduced.

2) We found that the scale of a cascading failure follows a power low distribution, i.e., a *long tail* is expected. This observation is in consistent with existing works, such as [14]. For instance, in Fig. 3(a), we notice that at $time = 0.19seconds$ and $time = 0.2seconds$, load 2 and load 5 are always affected, and the result keeps unchanged even with longer simulation time, such as $time = 0.3seconds$ (which is not shown). Compare the result with Fig. 1(a) which shows the topology of the Green Hub, it is not difficult to find that load 2 and load 5 are the loads which are closest to the initial fault, i.e., load 1. This suggests the possible existence of a critical distance, below which all connected loads will always be impacted. While we left the identification and verification of such a distance as one of our future work, an intuitive explanation is that the distance is short enough to allow the fault to propagate to the affected loads before the protective devices (relay, circuit, etc) are able to react. This result bring merits in that it might be very difficult to extinguish small scale cascading failure, and therefore it might be more benefit to shift our effort to forestall large scale blackout.

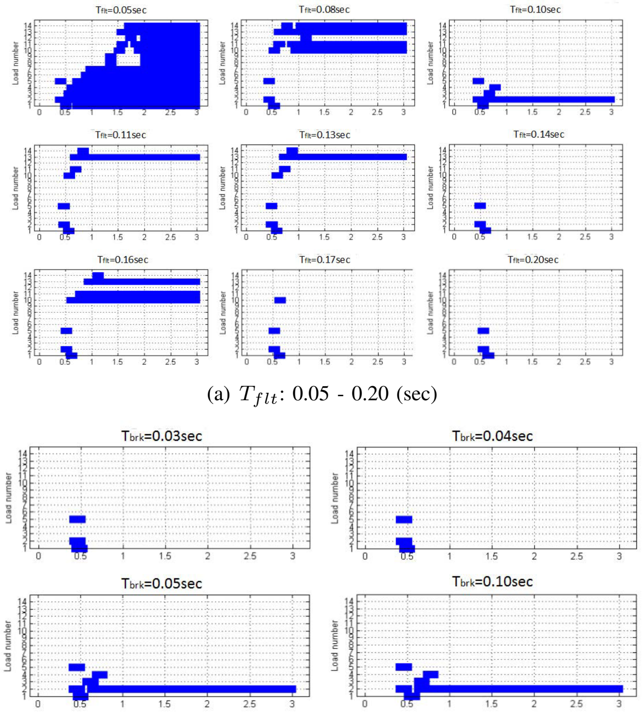
3) It is an interesting and counter intuitive observation that the scale of a cascading failure does not show monotonicity as we keep increasing a parameter's value. Instead, we observe a "gap" for both parameters. In parameter snapshot it is displayed as at some step, a snapshot shows a significant change from previous one, but the trend terminates at next step. Examples are as shown by the snapshot $time = 0.16seconds$ in Fig. 3(a), and $time = 0.07$ in Fig. 3(b). The gap is much clearer shown in parameter contour, where a dark-blue "canyon" splits the contour into two parts.

This observation conveys a positive information by indicating that achieving a sub-optimal solution could be much easier than that of optimal. Take Fig. 3(b) for example. A shorter break trip time (e.g., $T_{brk} = 0.03sec$) can reduce the impact of a cascading failure to the minimum, on the other hand, however, it requires devices with better performance, which usually indicates a higher cost. But this requirement could be much loosen if we aim at achieving a sub-optimal solution, such as we allow 4 loads to be fault as when $T_{brk} = 0.07sec$ instead of 3 which is optimal at $T_{brk} = 0.03sec$.

C. Cascading failure in communication enabled smart grid

Smart grid lays a communication network over traditional power grid, which makes it possible for devices to exchange information such as a fault message. As shown in Fig. 4, a cascading failure takes a few seconds to complete, which is more than enough for devices to exchange critical information, considering message transmission delay in communication networks is usually in milliseconds level. As a preliminary study of the smart grid, here we assume a simple communication scenario, in which a faulted device only disseminate this information to its neighbors.

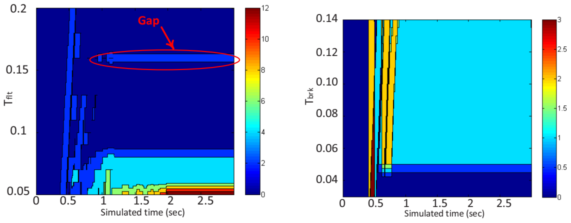
1) Simulation setup: Based on previous observation that load 2 and load 5 are always affected by the fault happened



(a) T_{flt}: 0.05 - 0.20 (sec)

(b) T_{brk}: 0.03 - 0.12 (sec)

Fig. 5. Parameter snapshot for T_{flt} and T_{brk}, with communication enabled.



(a) T_{flt}: 0.05 - 0.20 (sec)

(b) T_{brk}: 0.03 - 0.12 (sec)

Fig. 6. Paramter contour for T_{flt} and T_{brk}, with communication enabled.

on load 1, here we assume load 1 is able to send the fault information to load 2 and load 5 *as soon as load 1 sense the overcurrent*. On receiving this information, load 2 and load 5 change their tripping strategy from "delayed trip" to "instantaneous trip", which means $T_{brk} = 0$ on both load 2 and load 5, while other parameters' value keep unchanged. Results of this setup are shown in Fig. 5 and Fig. 6.

2) Observation and discussion: The simulation results are beyond our expectation. We observe a significant improvement for both simulations, in which the number of finally tripped load reduces to less than 5 or even down to 0 for all parameter values. This result fortifies the existence of smart grid, by showing that *when communication is enabled on power devices, a proper yet simple reaction could prevent a disaster from happening*.

We also find that the long-tail and gap are not obvious in both simulations. For Fig. 5(a) and Fig. 6(a) where we vary T_{flt}, the "gap" still exists at $time = 0.16 seconds$, however, the "long-tail" no longer exists (load 2 and load 5 is intentionally tripped therefore we do not take them into account); in Fig. 5(b) and Fig. 6(b) where we vary T_{brk}, we do not observe either "gap" or "long-tail".

V. Conclusions

We quantitatively evaluate the benefit brought by the communication enabled smart grid, in terms of how much it contributes in alleviating the aftermath of a disastrous cascading failure. To facilitate the evaluation, we propose a new cascading failure model, which is built in a real time power system simulator, and consider overcurrent as the root cause of failure, which is more realistic than generic overload assumption. Based on the new cascading failure model, three aspects regarding cascading failure, *time*, *space*, and *scale*, are studied. Our numerical results demonstrate that in smart grid, i.e., the communication enabled power grid, even a basic information exchange within limited devices can notably reduce the significance of a cascading failure. As our future works, we will measure practical communication delay using real devices [17], and incorporate the results into PSCAD simulation; and we will also leverage this work by taking advantage of cross-domain simulations [18].

References

[1] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," in *Proc. of IEEE MILCOM*, 2010, pp. 1830–1835.

[2] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[3] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, 2000.

[4] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman, "An initial model for complex dynamics in electric power system blackouts," in *Proc. of IEEE HICSS*, 2001, pp. 51–51.

[5] J. Chen and J. Thorp, "A reliability study of transmission system protection via a hidden failure DC load flow model," in *Proc. of IET Power System Management and Control*, 2002, pp. 384–389.

[6] "PSCAD," https://hvdc.ca/pscad/.

[7] S. Mei, M. Cao, and X. Zhang, *Power grid complexity*. Springer, 2011.

[8] N. S. Group, "Technical analysis of the august 14, 2003, blackout: What happened, why, and what did we learn?" 2004.

[9] P. Holme, "Edge overload breakdown in evolving networks," *Physical Review E*, vol. 66, no. 3, p. 036119, 2002.

[10] P. Holme and B. J. Kim, "Vertex overload breakdown in evolving networks," *Physical Review E*, vol. 65, no. 6, p. 066109, 2002.

[11] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, p. 065102, 2002.

[12] I. Dobson, J. Chen, J. Thorp, B. A. Carreras, and D. E. Newman, "Examining criticality of blackouts in power system models with cascading events," in *Proc. of IEEE HICSS*. IEEE, 2002, pp. 10–pp.

[13] I. Dobson, B. A. Carreras, and D. E. Newman, "A probabilistic loading-dependent model of cascading failure and possible implications for blackouts," in *Proc. of IEEE HICSS*. IEEE, 2003, pp. 10–pp.

[14] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *IEEE Trans. on IJEPES*, vol. 28, no. 9, pp. 627–633, 2006.

[15] "Wikipedia: Northeast blackout of 2003," http://en.wikipedia.org/wiki/Northeast_blackout_of_2003.

[16] "Distribution System Feeder Overcurrent Protection," http://www.geindustrial.com/publibrary.

[17] M. Wei and W. Wang, "Toward distributed intelligent: A case study of peer to peer communication in smart grid," in *Proc. of IEEE GlobeCom*, 2013, pp. 2210–2216.

[18] ——, "Greenbench: A benchmark for observing power grid vlunerability under data-centric threats," in *Proc. of IEEE InfoCom*, 2014, pp. 2625–2633.