

Dominoes with Communications: On Characterizing the Progress of Cascading Failures in Smart Grid

Mingkui Wei
North Carolina State University
Raleigh, NC, 27606

Zhuo Lu
University of Memphis
Memphis, TN, 38152

Wenye Wang
North Carolina State University
Raleigh, NC, 27606

Abstract—Cascading failures are one of the most devastating forces in power systems, which may be initially triggered by minor physical faults, then spread with Domino-like chain-effect, resulting in large-scale *blackout*. How to prevent cascading failures becomes imperative, as our daily lives heavily depend on stable and reliable power supply. The next-generation power system, namely *Smart Grid*, is envisioned to facilitate real-time and distributed control of critical power infrastructures, thus effectively forestalling cascading failures. Although cascading failures have been well investigated in the literature, most studies were confined only in the power operation domain with the assumption that communication is always perfect, which is, however, not true for today's communication networks, where traffic congestion and random delay happen. Therefore, an open question is *how to characterize cascading failures in the communication-assisted smart grid?* To this end, we take an in-depth inspection of cascading failures in smart grid and reveal the interactions between the power system and the communication network. Our results provide insights into the interactions between physical failure propagation and communication message dissemination. In addition, we show that while ideal communications can undoubtedly help prevent cascading failures, under-achieved communications (i.e., communications with severe delay) can, counter-intuitively, exacerbate cascading failures.

I. INTRODUCTION

A *cascading failure* refers to a large-scale power device outage, which is usually initiated by small-scale or even single device failure. Due to untimely or incorrect handling, it can spread along transmission lines in power grids, and cause much more devices to fail because of overloading. Repeatedly, those failed devices serve as new failure sources and propagate further, thus leading to devastating impacts and severe causalities. Recent studies on power grids revealed that in both the 2003 US-Canada blackout [1] and the 2012 India power outage [2], the initial and minor physical faults were neglected, and the subsequent *cascading failures* became rampant and overwhelming, which confirms that there is an urgent need to revamp the legacy monitoring and control systems to scale down, if not to eliminate, similar incidents in the future. Such a demand in essence suggests integrating advanced communications into next-generation power grid systems, i.e., Smart Grids [3], [4], which are envisioned to have real-time and distributed control of critical power infrastructures.

As our daily lives rely more and more on uninterruptible power supply, it becomes even more imperative nowadays

to combat all anomalies in power grids and facilitate a more reliable system than ever. Therefore, how to prevent cascading failures has received tremendous attentions [3], [5], [6]. Emerging smart grids, i.e., communication-assisted power grids, could be a life-saver towards forestalling cascading failures. For example, a relay (i.e., a device to sense a fault, and trip the circuit breakers surrounding the faulted part), can send its local information to neighboring relays, which will expedite those relays to make a global decision and take optimal actions before a physical failure arrives. Hence, there is no doubt that the concept of the smart grid is compelling and prospective.

Promising as it is, the smart grid can be implemented only after its benefits and drawbacks have been thoroughly studied. In this regard, unfortunately, we find that most existing studies on cascading failures only focus on evaluating the aftermath of blackouts (e.g., lost load and disconnected transmission lines) in the power grid domain only [7]–[9]. Although this line of work provides valuable insights on understanding the characteristics of cascading failures, they have two limitations. First and foremost, existing work does not explicitly assume the presence of a communication network. For example, the *load shedding* algorithm is used in many cascading failure models, in which each bus sheds a certain amount of load by itself in order to stop a cascading failure. In most existing models, load shedding is simply assumed to be taken by all buses without any consideration on how it is implemented. In fact, the load shedding decision is computed based on the global system information, and executed with the cooperation of all buses, which is impossible to be achieved without a communication network to carry all necessary message exchanges. Second, the consequence of a cascading failure is only *posterior-knowledge*. This is not sufficient to provide guidance on how to prevent or stop cascading failures, which requires more detailed information during the course of a failure propagation process, such as *which device* has experienced failure, *what* the cause is, and *when* the failure happens.

Therefore, a critical hurdle in fully embracing the smart grid is to understand the behavior of cascading failures in the power grid *with communications*, or in particular, to *characterize the progress of cascading failures in the communication-assisted smart grid*. Motivated by this question, we take in-depth investigation of the interactions between the power grid and the communication network and reveal the evolution of cascading failures in *practical* communication networks in

which packet losses and message delays exist.

Our contributions in this paper are three-fold. First, we take an in-depth inspection of the progress of a cascading failure in smart grid by considering the reactions taken in both the power grid and the communication network. Second, we define three new metrics to characterize the progress in finer granularity, which are, *overload lines*, *island lines*, and *total outage lines*. These metrics can clearly indicate the significance of a cascading failure, and also profile its evolution. Third, we study the impact of imperfect communications on stopping a cascading failure, and show that compared with the scenario in which the assistance of communications is absent, a severely under-achieved communication can, counter-intuitively, exacerbate the consequence and cause even more failures.

The remainder of this paper is organized as follows. In Section II, we introduce the backgrounds. In Section III, use an example to reveal the progress of cascading failures in the communication-assisted smart grid. In Section IV, we provide the details of our simulations and analysis. Finally, we conclude our work in Section V.

II. BACKGROUNDS AND RELATED WORKS

In order to study the cascading failure, the power grid is usually modeled as a graph, in which the edges and vertices denote the transmission lines and power substations (buses) in the power system, respectively. Each bus is associated with either power consumers (loads) or power providers (generators), and each line carries power between generators and loads in order to achieve system equilibrium. The amount of power carried (power flow) on each line can be calculated by using either Direct Current (DC) model [10], [11] or Alternating Current (AC) model [12], both of which are approximations to power systems in the real world. Between the two, the DC model is more preferred by most researchers especially in cascading failure study, because it provides better balance between computational complexity and approximation accuracy.

A cascading failure can be triggered by the failure of one or more lines in the power system. Particularly, when a line fails, the power needs to be redistributed on all remaining lines in order to regain system balance, which will cause power flow to change on these lines. As a result of the power redistribution, the power flow on some lines may exceed their threshold, and cause those lines to fail. Those newly failed lines serve as a new failure source and further cause more lines to overload and fail, and the domino-like cascading failure is formed.

In order to relieve overloaded lines and prevent them from failure, load shedding is a common method to be applied [10]. Load shedding is to sacrifice by self-disconnecting a portion of load on all buses to eliminate overload on transmission lines, which is a complicated problem by itself and has been studied by many researchers [9]–[11], [13]. For the purpose of cascading failure study, the load shedding is usually formulated as a linear programming problem [9]–[11], in which the objective is to keep the cost of load shedding as low as possible, while eliminating overload on all lines.

III. UNDERSTANDING THE PROGRESS OF CASCADING FAILURES IN SMART GRID

In Fig. 1 we take a 4-bus power system as an example to demonstrate the progress of cascading failures in the communication-assisted smart grid. As plotted in Fig. 1, the smart grid is composed by two counterparts, the cyber system, i.e., the communication network, and the physical system, which is the power grid. This figure shows 4 critical steps during the progress of a cascading failure in the smart grid, and each step is depicted by 2 subfigures in both the cyber system and the physical system, shown as the subfigures above and below the time line. In the following description, we use C1-C4 and P1-P4 to denote subfigures of the cyber and physical systems at steps 1-4 illustrated in Fig. 1, respectively. For instance, subfigure P1 refers to the bottom-left subfigure which denotes the event that happens in the physical system at step 1, and C1 refers to the top-left subfigure which denotes the event that happens in the cyber system at step 1.

A. Assumptions and Denotations

In order to facilitate our explanation of the progress of cascading failures in smart grid, we first make the following assumptions and denotations about this cyber-physical system.

1) *The power system*: The power system shown in Fig. 1 is composed of 4 buses and 5 transmission lines, which are denoted by $b_i, i \in \{1, 2, 3, 4\}$ and $l_j, j \in \{1, 2, 3, 4, 5\}$, respectively. We define the *state* of the power system, denoted by S , a 1×5 vector whose element s_j denotes the status of line l_j . Particularly, $s_j = 1$ if l_j still exists in the power system, and $s_j = 0$ if l_j has failed and been removed from the system. The state of a power system will change over time, and we use S_k ($k=1, 2, \dots$) to denote its k -th state.

2) *The communication network*: In the smart grid, each bus is equipped with a control unit, which implements the function to monitor the status of the bus and adjacent lines, control bus activities, and most importantly, communicate with control units on other buses. We use $\{h_i\}, i \in \{1, 2, 3, 4\}$ to denote these communication *hosts*.

We assume there are two types of control units in the smart grid. The *Intelligent Electronic Devices (IEDs)* are lower-end computers which can only monitor and control a bus and communicate with other hosts. And the *Control Centers (CCs)* are powerful computers, besides the basic monitoring, control and communication, it collects information from adjacent IEDs, executes calculations and makes load shedding decisions during a cascading failure.

3) *Cascading failure initialization*: As introduced in Section II, cascading failures are initialized by a random failure and removal of one transmission line. And the spread of the cascading failure is caused by overloaded lines caused by previously failed lines. We denote the power flow on line l_j as f_j , and the threshold of the power flow as \hat{f}_j .

B. The Progress of Cascading Failures

Step 1: Cascading failure initiation.

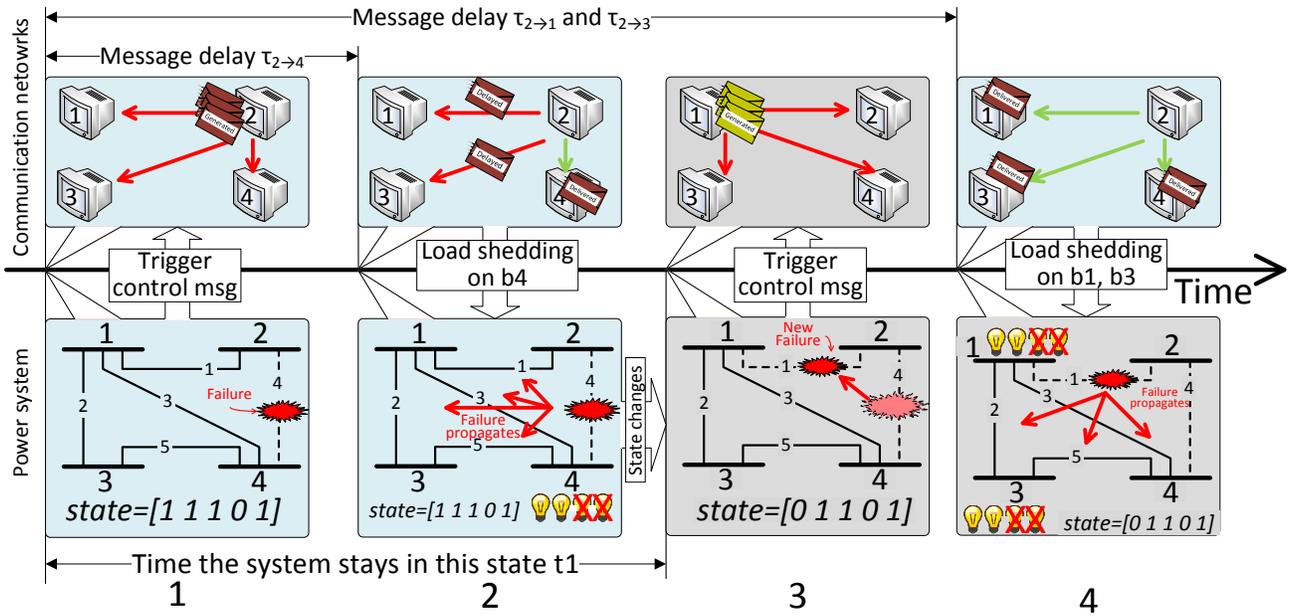


Fig. 1. Because messages from host 2 (h_2) to h_1 and h_3 are delivered later than physical fault arrives at line 1, the cascading failure is not stopped.

A cascading failure is initiated by a random line failure in the power system. As shown in subfigure P1 in Fig. 1, assume that a trigger failure is on l_4 . Right after l_4 failed and be removed from the power system, two events happen in both domains.

- 1) In the power system, as shown by subfigure P1, the removal of l_4 breaks the system equilibrium, i.e., the power which flew on l_4 needs to be redistributed on all other remaining lines. This power redistribution may cause the power flow on some lines to exceed their threshold, and cause these lines to fail.
- 2) In the communication network, as shown by subfigure C1, the failure of l_4 is detected by h_2 , which is a control center. On knowing the failure, h_2 runs the calculation and makes the decision to shed load on b_1 , b_3 , and b_4 , which reduces the overall power demand in the system and therefore makes sure the power flows on all remaining lines will not exceed their threshold.

Step 2: Load shedding partially takes place.

As shown in subfigure C2, h_4 receives the load shedding command from h_2 in this step, then executes the load shedding command and disconnects some load from bus b_4 , as shown by subfigure P2.

At this time, in the communication network, the messages from h_2 to h_1 (denoted as $m_{2 \rightarrow 1}$) and h_3 (denoted as $m_{2 \rightarrow 3}$) are still in transmission and have not been received. And in the power system, the power flow on the remaining lines begins to change, because the power flow changes gradually over time, there is not any line which has experienced overload yet.

Step 3: Cascading failure propagates.

If the messages from h_2 can be delivered to all other hosts, and load shedding on all buses can be executed, the power flow

on all remaining lines will remain within their threshold, and eventually no further failure will happen. However, because the message $m_{2 \rightarrow 1}$ and $m_{2 \rightarrow 3}$ are not delivered on time, cascading failure propagates as shown in step 3.

As shown by subfigure P3, the power flow on line l_1 passes its threshold before $m_{2 \rightarrow 1}$ and $m_{2 \rightarrow 3}$ are delivered. As a result, l_1 fails and is removed from the system, which triggers another load shedding message dissemination event (shown in subfigure C3, which is similar to subfigure C1).

Step 4: Delayed message delivery.

Messages $m_{2 \rightarrow 1}$ and $m_{2 \rightarrow 3}$ are eventually delivered in step 4, and the load is shed on buses b_1 and b_3 . However, it is too late and the failure propagation cannot be stopped, because the new failure on l_1 has been added to the original l_4 failure, which means that more load needs to be shed in order to regain system balance. And also as shown in subfigure P4, the new failure happened at line l_1 will cause further power flow change on lines l_2 , l_3 , and l_5 . Depending on whether the messages generated in subfigure C3 will be delivered on time or not, the cascading failure may propagate even further.

C. Characterizing the progress of a cascading failure

In Fig. 1, we see that the propagation of a cascading failure essentially depends on whether the messages can be delivered before a new physical fault is caused. Therefore, we define the *message delivery rate* to characterize the race between message dissemination and fault propagation.

Definition 1: (Message delivery rate).

Given a smart grid with n buses and hosts, the *message delivery rate*, denoted as $\gamma_{i \rightarrow j, \Delta k}$, is the probability that the

message generated in k -th state of the power system will be delivered in the $(k + \Delta k)$ -th states, which is defined as

$$\gamma_{i \rightarrow j, \Delta k} = P(\tau_{i \rightarrow j} < \sum_{x=k}^{k+\Delta k} t_x), \forall i, j \in [1, n], \Delta k \in \mathbb{N}, \quad (1)$$

where Δk denotes elapsed number of states, $\tau_{i \rightarrow j}$ is the delay of the message sent from host h_i to host h_j , and t_x is the time interval the power system stays at state x .

For example, $\gamma_{i \rightarrow j, 0}$ is the probability that the message can be delivered before any other failure is caused in the system, and $(\gamma_{i \rightarrow j, 1} - \gamma_{i \rightarrow j, 0})$ means the message is delivered after the first failure but before the second failure is caused.

D. Evaluating the result of a cascading failure

In order to evaluate the significance of a cascading failure, we define three metrics to measure the significance of a cascading failure during each state.

Definition 2: (Overload, island, and total outage lines).

Given a smart grid with m transmission lines, the *overload lines*, denoted by L_O , is the set of transmission lines that have been removed because the power flows on them have exceeded their threshold, which is defined as

$$L_O = \{l_j | f_j > \hat{f}_j, j \in [1, m]\}. \quad (2)$$

The *island lines*, denoted by L_I , is the set of transmission lines that do not overload, but are eventually isolated from any generator because all adjacent lines which connect it to a generator have been removed. The set of island lines is defined as

$$L_I = \{l_j | f_j \triangleq 0, j \in [1, m]\}, \quad (3)$$

where $f_j \triangleq 0$ means that the power flow through line j is *always* zero because all lines that connect it to any generator have failed.

And the *total outage lines*, denoted by L_T , is the set of transmission lines that have failed due to either overload or island, which is defined as

$$L_T = L_O \cup L_I. \quad (4)$$

E. Discussion

In most existing works on cascading failure study, only the number of the total outage lines, i.e., $|L_T|$, is evaluated, which is insufficient to depict the details of how cascading failure progresses. The three metrics defined in this paper take snapshot for each state change during the process of a cascading failure, which can not only reflect how many lines have been failed, but also show which lines experienced failure and what is the reason of the failure. Those indications are more meaningful, because knowing the number (e.g., $|L_T|$) only provides *posterior-knowledge* of the consequence of a cascading failure; in contrast, knowing exactly which lines are vulnerable can provide empirical suggestions to system scheduling and maintenance, such as improving the tolerance on weak lines, or even adding more lines to offload the pressure and reduce the failure probability.

IV. SIMULATION SETUP AND RESULTS

A. System Setup

In this section, we use a case study to evaluate the progress of cascading failures in smart grid based on the observations we made from Section III. In particular, we build a small-scale smart grid prototype, namely the Green Hub, which is a 18 bus system with 24 transmission lines, to study the process of a cascading failure in the communication-assisted smart grid. The topology of the Green Hub is omitted due to page limit, interested readers can refer to our previous work for more detailed information [14].

1) *Line threshold \hat{f}_j* : It is clear that the larger the threshold compared with its normal operation value, the less likely a cascading failure will happen. However, larger threshold on the other hand means higher investment on better quality of transmission lines and a waste of the unused capacity. In practice the threshold is usually set to be at most 1.2 times of a line's normal operation value. In our study we tested \hat{f}_j ranging from 1 to 1.2 times of f_j and find that both extreme values tend to make the result indistinguishable; i.e., if it is too small, any trigger failure will eventually cause all line to fail, while if it is too large, hardly any line will exceed threshold and fail, and both scenarios are difficult for us to observe the impact of varying communication conditions. Therefore, we chose $\hat{f}_j = 1.1$ times of its normal operation value in this case which provides well-distinguishable results.

2) *State holding time of the power system t_x* : As shown by the demonstration in Section III, to study the progress of a cascading failure, it is critical to find out the time period between two continuous physical failures, i.e., state holding time. To our best knowledge, there exists no work studying or modeling such a time period. Therefore, in our study, we build a power system in real-time power system simulator and find the time via simulations.

In particular, we build the Green Hub in PSCAD [15], a real-time power system simulator, and collect the fault propagation time by conducting multiple runs. In each run, we first start the simulation and wait until the system enters stable state, then we disconnect one line and record the time when power flow on other lines exceeds \hat{f}_j , and use this as one sample. We conduct this simulation for all 24 lines in the system and empirically fit the collected sample data to a log-normal distribution with parameter $\mu = 1.3292$, $\sigma = 1.5504$.

3) *Message delay $\tau_{i \rightarrow j}$* : The delay of a message in a communication network can usually be modeled as a random variable. In order to better understand the impact caused by each individual factor, we assume the delay is a constant, i.e., $\tau_{i \rightarrow j} = c, \forall i, j$ in the first part of our case study, and we abandon this assumption in later study and observe the impact caused by varying message delays.

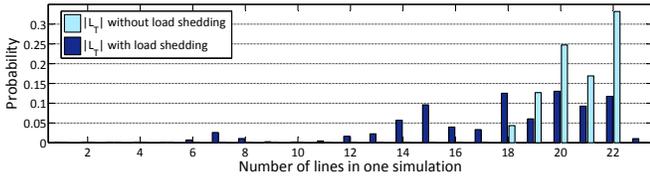
To find a proper value for $\tau_{i \rightarrow j}$, we take reference from the IEC 61850 standard [16], which is a standard that defines communication requirements in smart grid communication. In the IEC 61850 standard, it is specified that the most critical messages, such as commands to trip a circuit breaker, should

be delivered within 3 ms. We assume that $\tau_{i \rightarrow j} = 3ms, \forall i, j$ such that we can observe the physical system's reaction when the cyber system is "well-behaved".

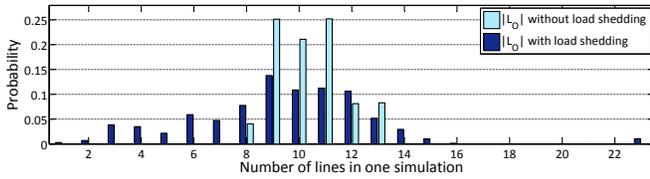
For simplicity, we also require the message does not pass more than 2 states, i.e., if $\tau_{i \rightarrow j} > \sum_{x=k}^{k+2} t_x$ then set $\tau_{i \rightarrow j} = \sum_{x=k}^{k+2} t_x$. For instance, if a message was issued in state 1 and the power system has evolved to state 3, the message will be delivered before the power system evolves to state 4 anyway.

B. Simulation Setup and Results

The simulation of each scenario consists of 10,000 runs and the results are aggregated. At the beginning of each simulation, we randomly choose one line as the trigger failure and remove it from the power system. Per each simulation, we record L_O , L_I , and L_T at the completion of the cascading failure.



(a) $|L_T|$: with load shedding vs. without load shedding.



(b) $|L_O|$: with load shedding vs. without load shedding.

Fig. 2. $|L_O|$ and $|L_T|$: with load shedding vs. without load shedding.

In Fig. 2 we plot the probability distribution of $|L_O|$ and $|L_T|$ for two scenarios. The light blue colored bars denote the scenario without communications, where no load shedding strategy is applied (i.e., the cascading failure progresses without any remediation); and the dark blue colored bars denote the scenario with communication where load shedding is present. L_I is neglected as it can easily be deduced by L_O and L_T .

We first look at $|L_O|$ in both scenarios in Fig. 2(b). As shown by the light blue bars, when load shedding is not present, the number of overload lines as a result of a cascading failure ranges from 8 to 13. The peaks locate at $|L_O| = 9, 10, 11$, which means on average, there are 9-11 lines that are very susceptible to cascading failure.

We compare the two sets of colored bars by dividing them into 3 sections, $|L_O| \in [1, 8], [9, 13], [14, 23]$. Compared with the light blue bars, it is clear that the dark blue bars are much lower in the 2nd section, but have been significantly increased in the 1st section. This is an indication that with communication, the significance, i.e., how many lines will fail, of cascading failure has been reduced, however, the total number of events does not decrease noticeably, which can be calculated by summing the value of all bars. Therefore, communications help in *alleviating* cascading failures rather *eliminating* them.

The most interesting yet counter-intuitive result lies in the 3rd section, particularly at $|L_O| = 14, 15, 23$. As shown in Fig. 2(b), the load shedding makes more severe events happen, which does not exist when load shedding is not applied, which suggests *the presence of communication and load shedding may exacerbate the consequence of a cascading failure*. The cause of this phenomenon may be explained by the accumulation of errors: because some load shedding commands are not delivered on time, corresponding lines that should have been disconnected still remain in the system. This keeps accumulating and can finally cause an avalanche and exacerbates the failure situation.

When we look at the event from the whole system perspective by considering $|L_T|$ as shown in Fig. 2(a), however, we find the load shedding, although not perfect, does help alleviate the consequence of a cascading failure. The probability of $|L_T| = 22$ is reduced by more than 20%, while $|L_T| = 21$ and $|L_T| = 20$ are also less likely to happen.

Our speculation that there may be 9 - 11 lines that are vulnerable and needed to be improved is supported by Fig. 3, in which we plot the number of outages for each line during the 10,000 simulations. Several observations can be made:

i). In the system level, load shedding helps alleviate the consequence of a cascading failure. For example, without communication, there are 9 lines (light blue bars) whose failure counts exceed 6,000; but with the presence of communication, this number reduces to 5 (dark blue bars).

ii). Load shedding does not grant unanimous fairness on all lines. For instance, although most of the light blue bars have been shortened, bars 1 and 8 are actually prolonged, which means lines 1 and 8 suffer larger failure probability than that without communication.

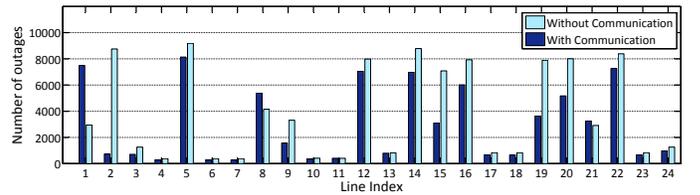


Fig. 3. Summation of L_O in 10,000 simulations.

C. Exploration of Message Delivery Rate

According to the definition of $\gamma_{i \rightarrow j, \Delta k}$, we can find its value with the given distribution of the power system state holding time t_x , especially when we assume that $\tau_{i \rightarrow j}$ is fixed. In particular, $\gamma_{i \rightarrow j, 0} = P(\tau_{i \rightarrow j} < t_k) = F_{t_x}(t = \infty) - F_{t_x}(t = 3ms) = 0.56$, and $\gamma_{i \rightarrow j, 1} = P(\tau_{i \rightarrow j} < 2t_k) = 0.72$, and because we assume all messages are delivered no later than the second passed state, we have $\gamma_{i \rightarrow j, 2} = 1$. This means that for a message, the probability that it will be delivered before any new failure is 56%, the probability that it will be delivered after the first failure but before the second failure is 16%, and the probability it can be delivered after the second failure is 28%.

We see that the message delivery rate plays a critical role in stopping a cascading failure. Intuitively, the larger the value of $\gamma_{i \rightarrow j,0}$, the better the performance; and in the ideal case, if all messages can be delivered before any failure is caused, i.e., $\gamma_{i \rightarrow j,0} = 1$, no failure will be caused and the cascading failure is completely prevented. In this subsection, we explore the impact of cascading failures under different communication conditions by varying $\gamma_{i \rightarrow j,0}$.

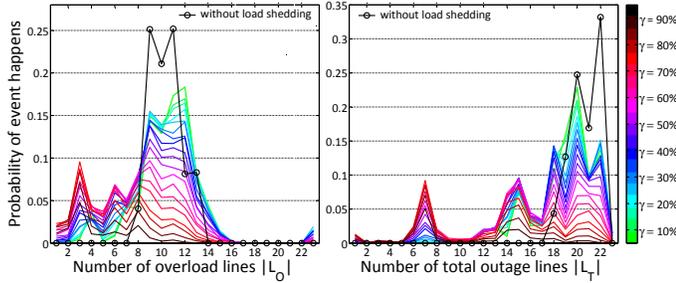


Fig. 4. Variation of $|L_O|$ and $|L_T|$ with $\gamma_{i \rightarrow j,0}$ transiting from 5% to 100%, different colors represent simulation result of different $\gamma_{i \rightarrow j,0}$.

We run multiple simulations by varying $\gamma_{i \rightarrow j,0}$ from 5% to 100% with 5% each step while keep $\gamma_{i \rightarrow j,1} = \gamma_{i \rightarrow j,2} = 0.5(1 - \gamma_{i \rightarrow j,0})$, and plot the transition of $|L_O|$ and $|L_T|$ in Fig. 4. As shown by Fig. 4, each subfigure contains 19 lines with different colors indicated by the colorbar on the right, among which each colored line denotes one particular communication condition. For instance, the lightest-green line shows the result of $|L_O|$ and $|L_T|$ when the probability that a message can be delivered on time is only 5%.

Several observations can be drawn from Fig. 4.

i) Improved communications do not eliminate cascading failure, but only alleviates its consequence. As shown by both subfigures, with $\gamma_{i \rightarrow j,0}$ increasing, the peak of the lines is not suppressed but gradually moved toward left, meaning although the probability of more significant cascading failures has been reduced, less significant ones appear more frequently.

ii) Inspecting the right subfigure, we see even severely delayed messages can still help alleviate the consequence. For instance, the probabilities of $|L_T| = 21, 22$ of green-color lines ($\gamma_{i \rightarrow j,0} = 5\% - 15\%$) are much smaller than that without communication, which is shown by the black-circle line.

iii) Communications may cause more lines to overload and fail. For instance, as shown in the left subfigure, when the message delivery rate is under 50%, which is depicted by the set of light green to dark blue lines, the probabilities of $|L_O| = 12, 14, 15$ are much larger than those without load shedding, which means with under-achieved communication, cascading failures can more likely lead to more overloaded lines.

D. Discussion

One of our major observations is that counter-intuitively, load shedding with under-achieved communication performance can increase the possibility of more serious blackouts. This phenomenon, however, is not singular and can be found in many other areas. In [17], [18], authors gave a “forest fire

model”, which shows that the effort spent on extinguishing small-scale fire in a forrest actually increases the probability of large-scale conflagration. Authors in [17] further show that, if we assume that the power grid can tolerate a certain number of small-scale failures, e.g., remove lines from the system only when there are more than 3 lines that are overload instead of 1, from a long time perspective the result is actually worse. These are effective reminders for system planners that *a seemingly beneficial solution might just be a buried hazard, which may accumulate and cause avalanche failures as time goes by.*

V. CONCLUSION

We take an in-depth inspection of the progress of cascading failures in smart grid by examining the race between message dissemination in the communication network and fault propagation in the power grid. To our best knowledge, it is for the first time, cascading failures are inspected by accounting for both communications and power management schemes. We find that communications may hinder load shedding in accomplishing its objective, and might further exacerbate its consequences, which suggests that minimizing the communication delay is critical in avoiding large-scale blackouts.

REFERENCES

- [1] “U.S. - Canada power system outage task force: Final report on the implementation of task force recommendations,” <http://energy.gov/>.
- [2] “2012 India blackouts,” <http://en.wikipedia.org/>.
- [3] Office of the National Coordinator for Smart Grid Interoperability, “NIST framework and roadmap for smart grid interoperability standards, release 1.0,” *NIST Special Publication 1108*, 2009.
- [4] H. Farhangi, “The path of the smart grid,” *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.
- [5] The SG Interoperability Panel - Cyber Security Working Group, “Smart grid cyber security strategy and requirements,” *NIST IR-7628*, 2010.
- [6] M. Wei and W. Wang, “Combat the disaster: Communications in smart grid alleviate cascading failures,” in *IEEE HONET*, 2014, pp. 133–137.
- [7] J. Yan, Y. Zhu, H. He, and Y. Sun, “Revealing temporal features of attacks against smart grid,” in *Proc. of IEEE PES ISGT*, 2013.
- [8] I. Dobson, B. A. Carreras, and D. E. Newman, “Branching process models for the exponentially increasing portions of cascading failure blackouts,” in *Proc. of IEEE HICSS*, 2005.
- [9] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, “Power grid vulnerability to geographically correlated failures – analysis and control implications,” in *Proc. of IEEE INFOCOM*, 2014.
- [10] 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.
- [11] 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.
- [12] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, “Criticality in a cascading failure blackout model,” *International Journal of Electrical Power & Energy Systems*, vol. 28, no. 9, pp. 627–633, 2006.
- [13] K. U. Rao *et al.*, “A novel grading scheme for loads to optimize load shedding using genetic algorithm in a smart grid environment,” in *Proc. of IEEE ISGT Asia*, 2013, pp. 1–6.
- [14] M. Wei and W. Wang, “Greenbench: A benchmark for observing power grid vulnerability under data-centric threats,” in *Proc. of IEEE INFOCOM*, 2014.
- [15] “PSCAD,” <https://hvdc.ca/pscad/>.
- [16] IEC Standard, “IEC 61850: Communication networks and systems in substations,” 2003.
- [17] B. A. Carreras, V. E. Lynch, D. E. Newman, and I. Dobson, “Blackout mitigation assessment in power transmission systems,” in *Proc. of IEEE HICSS*, 2003, p. 10.
- [18] B. Drossel and F. Schwabl, “Self-organized critical forest-fire model,” *Physical Review Letters*, vol. 69, no. 11, p. 1629, 1992.