Domino of the Smart Grid: An Empirical Study of System Behaviors in the Interdependent Network Architecture

Xiang Lu, *Member, IEEE,* and Wenye Wang, *Senior Member, IEEE* and Jianfeng Ma, *Member, IEEE* and Limin Sun, *Member, IEEE*

***Abstract*—The smart grid features a unique network architecture that consists of two coupled and interdependent networks, including the communication network and the power network. The communication network serves as the infrastructure of information disseminations to deliver control commands and device running states for the power network, whereas the power network supplies the energy to support the communication network. Nevertheless, besides such an reciprocal relationship, the two coupled networks also bring more threats of cascading failures to the smart grid against the system reliability, which will be more serious in the situation that communication devices are installed with back-up power supplies. In this paper, we present a detailed review of the system architecture of the smart grid and investigate the complicated evolution process of iterative failures' propagations between the coupled networks. Our analysis claim that there exists a potential domino affect to make original power faults be propagated in a wide area. To testify our analysis, we design and implement a co-simulation framework to integrate the communication network simulation with the power network simulation. Through experiments, we quantify two critical metrics to indicate the possibility of the potential fault spreading in the smart grid. Our work replays the complicated network behaviors implied in the coupled network architecture and provides preliminary statistical results towards a fine-grained mathematical model to describe the interesting phenomenon of iterative fault propagations.**

***Index Terms*—Smart Grid, Interdependent Networks, Iterative Fault Propagation, A Co-simulation Framework.**

I. Introduction

THE smart grid is an emerging technology that leverages advanced information technologies to provide efficient, flexible and reliable electricity services. In the brand new power delivery paradigm, the most salient feature is two-way flows of electricity and information [1], in which, distributed electricity flows are accurately driven by real-time information flows to enable a near-instantaneous energy balance serving for dynamic supply and demand, thereby remarkably improving the energy efficiency. To achieve envisioned two-way flows of electricity and information, state-of-the-art communication and network technologies (e.g., Ethernet, WiFi, and TCP/IP) are being widely integrated into power systems [2] to facilitate interconnections of power devices towards ubiquitous device state acquisition and supervisory. Thus, a communication network comes out over the underlying power network to portray the smart grid in a two-layer network manner.

The unique architecture of the two-layer network in the smart grid recently attracts great research interests on the system reliability after the seminal work [3]. In [3], researchers modeled the power system as two coupled, yet interdependent networks: a communication network provides information delivery services to help control a power system, whereas a power system supplies power to energize the communication network. Then, the interdependent two-layer network was evaluated in a serious power outage, which further demonstrated a extreme sensitivity of the coupling, interdependent networks to random cascading failures. Hereafter, quite many works [4], [5], [6] dedicate their efforts to the modeling and evaluation of system robustness with interdependent multiple networks.

Although these models have thoroughly described potential cascading behaviors in interdependent networks, they are not enough to represent interoperations of the two-layer network in the smart grid. The reason lies in that all above models are based on one assumption, that is, the communication network becomes dysfunctional immediately once the power substations loss power. However, the assumption may not hold in practice, especially when mainstream routers start to be equipped with the back-up battery power [7], [8]. Moreover, there is even an online tutorial[1] to teach people how to manipulate the electrical circuit to power a base station using solar energy. Thus, it is conceivable that, it is not a big deal to ensure the communication network still working for a while after the power loss. If that is the case, existing results may not be applicable. It is necessary to re-investigate, *what role the communication network plays in the interdependent networks when cascading failures happen in the smart grid*. The answer to this question will benefit both electrical engineers and communication engineers: for the former, it will clarify potential performance affects brought by communication networks on the traditional power contingency analysis [9], which usually

X. Lu and L. Sun are with the Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China, 100093.
E-mail: luxiang@iie.ac.cn

W. Wang is with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh NC, 27606.
E-mail: wwang@ncsu.edu

J. Ma is with the Department of Computer Science, Xidian University, Xi'an, China, 710071.

This work was supported in part by the State Key Development Program for Basic Research of China (Grant No. 2011CB302902), the National High Technology Research and Development Program of China (Grant No. 2012AA050804), the State Key Program of National Natural Science of China (Grant No. 60933011), and the "Strategic Priority Research Program" of the Chinese Academy of Sciences (Grant No. XDA06040100).

[1] http://wiki.mikrotik.com/wiki/Solar_Power_HOWTO

supposes that the communication network is fault-free; for the latter, it will offer an intuitive understanding regarding the consequence of a communication fault in the power network when both networks are coupled together.

To characterize performance affects of the communication network on smart grid operations, in this paper, we firstly take a power distribution network as an example to analyze possible cascading failure behaviors implied in coupled networks. Our analysis reveals that, various delay-constrained message deliveries will result in non-neglected transmission failures in the communication network, which are further superimposed over original power faults to exacerbate situations of system reliability. In order to verify our analysis, we then design and implement a python-based co-simulation framework to cooperate the network simulation with the power-flow-analysis based power network simulation together. Through the co-simulation framework, we are able to observe details of the complicated iteration process towards first-hand statistical performance results, which will help us to model the cyber-power system in the next step. Our results show that, the failed message transmission will dramatically enlarge the original power fault as an amplification effect to destroy more nodes.

The rest of this paper is organized as follows. Section 2 describes the coupled networks and potential cascading failure behaviors in the power distribution system. In Section 3, we present the design and implementation of our co-simulation framework, including the communication part and the power part. Detailed experimental results are discussed in Section 4. Finally, we conclude this paper in Section 5.

II. Cyber and Power Coupled Networks

In this section, we firstly take a power distribution system as an example to introduce the aforementioned cyber-power coupled network architecture in the smart grid. Then, we illustrate how interdependent networks behave in a fault management operation in an intuitive way.

A. Coupled Network Architecture

Generally, a power system is a complex system connecting various power electronics devices from the power generators to customers through power transmission and distribution systems. As more and more renewable energy generators, such as solar panels and wind turbines, are widely envisioned in the future power distribution system [10], [11], it is becoming the research focus to achieve flexible energy sharing within a residential community, thereby forming the so-called "micro-grid" [12]. In the microgrid, distributed power generations are involved to supply neighboring loads and to allow local control to reduce or eliminate the need for central energy dispatching.

Fig. 1 shows a community map, where many distributed power generators are deployed to form a power distribution system. To monitor and control the distribution system, every power device is firstly attached with an intelligent electrical devices (IED) as an agent [13] to execute control missions according to device states. These agents are then interconnected to ensemble the communication network over the underlying power topology, in which, various device states are readily to

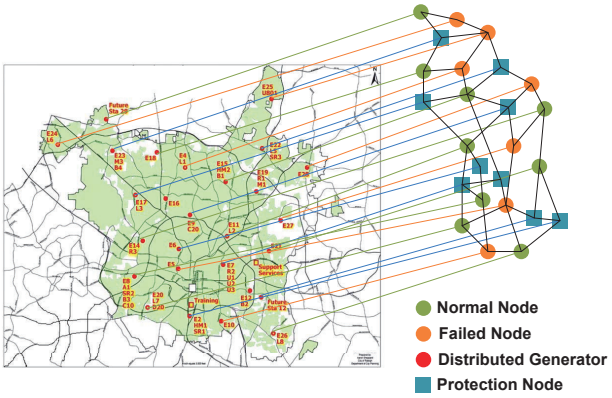

Fig. 1. Deployment of A Coupled Cyber-Power Network.

be exchanged towards a global system state detection. In this sense, two coupled networks are formed as follows:

Power Network: The underlying power devices, including transformers, generators and circuit breakers, are interconnected as peers for the electricity delivery. The connections between devices are composed of diversified feeders or transmission lines. The power network topology indicates how energy flows among power devices.

Communication Network: IEDs, also known as device controllers, are nodes in the communication network. They are networked through wired or wireless links [14] for exchanges of real-time equipment data and urgent alarms. Every IED is associated with the corresponding device node in the underlying power network. The topology of the communication network implies message delivery relations among IEDs that is different from the topology of the power network. Furthermore, links between communication nodes are determined by applications [15], [11]. For example, when an fault occurs due to a device malfunction, the alarm message is expected to be multicasted to multiple receivers to ensure a coordinated action between equipments [16]. Therefore, if multiple applications run on an IED, the IED needs to maintain multiple multicast groups for different applications, as shown in Fig. 2. When transmitting messages, IEDs firstly check the map to ensure the matched receivers in the multicast group. Then, different messages are multicasted to different destinations, thereby forming topologies of the communication network.

B. Interdependent Behaviors in the Fault Management

With the overlay network architecture, we then detail *how such two interdependent networks behave in applications of power management in the smart grid*. Without loss of generality, we take a fault management scenario as an example, which is the most common, as well as the most critical operation in the power system [17], aiming at the system reliability maintenance. Usually, such a kind of applications is trigged from a power device failure, like a transformer malfunction, and ends with a fault clearance by tuning states of corresponding devices, such as tripping, closing, or re-closing circuit breakers. However, the fault management system may not operate as expected due to inevitable communication

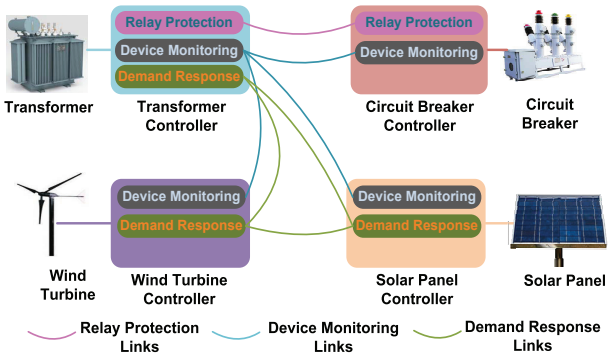

Fig. 2. Multicasted Application Message Maps in a Microgrid System.

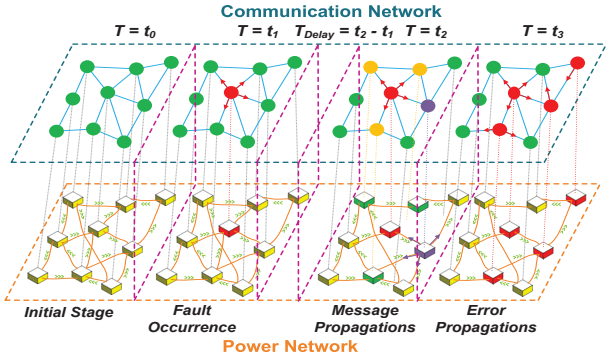

Fig. 3. Behaviors of interdependent networks in a fault management scenario.

failures in such an interdependent system. In this section, we highlight interdependent behaviors of two coupled networks within a fault management application, as shown in Fig. 3.

Initial Stage. In the beginning, $T = t_0$, the entire system runs normally.

Fault Occurrence. At $T = t_1$, a fault firstly happens in the power network as a transformer malfunction, or an overcurrent fault in a feeder. The abnormal state is then captured by the device and the associated IED, shown as the red dot in Fig. 3. The fault-aware IED node is ready to disseminate alarms for protection actions. After checking the multicast message map, the fault node starts to emit alarms in four directions.

Message Propagations. Since message deliveries are subject to rigorous timing requirements in the smart grid [11], alarm messages successfully arrive at receivers in three directions (denoted as yellow dots in Fig. 3) within the permitted propagation period T_{Delay}, but fail in one direction (denoted as a purple dot). Reasons of the unsuccessful delivery are diverse, such as time-consuming message processes [18], malicious jamming attacks [19], even network congestions [13]. Hence, at $T = t_2$, only three green-marked power devices whose attached IEDs receive alarms correctly. Furthermore, only those alarm-aware power devices will act towards a fault clearance operation, while those devices that miss the alarm may keep their states unchanged. Without the expected coordination, the original fault can not be cleared. Even worse, the alarm-missed device (marked as the purple one) is prone to be another fault source to damage nearby devices again.

Electricity Error Propagations. More devices will be damaged by the alarm-missed device, thereby increasing the number of fault devices from 1 to 4 in Fig. 3. Correspondingly, four associated communication nodes will be activated again to surge a new round of alarm propagation in a larger area. Therefore, a fault iteration forms. Such a fault iterations will finish as long as any one of the following condition is achieved: 1) the fault is cleared through device cooperations; 2) a blackout appears in the whole system.

Generally, we can claim that, the interdependent relationship between the coupled communication and power networks makes network behaviors more complicated. However, we can still partition the complex interdependent behaviors into two iterated processes, one is a time-limited message propagation in the communication network, which is triggered by the device fault of the power network; whereas the other is an electricity error dissemination in the power network, which can be seen as system responses to the message propagation of the communication network. Based on this understanding, we in the following sections replay the interesting interdependent phenomena using a co-simulation framework to explore open questions on reliability issues in the smart grid.

III. INDEPNETSIM: A CO-SIMULATION FRAMEWORK

To replay interdependent iterations of the cyber-power system towards detailed performance observations, we design and implement a python-based co-simulation framework to cooperate message transmissions in the communication network with electricity deliveries in the power network. We will firstly introduce algorithms used to simulate the communication network, then present methods of the power-flow-analysis based power network simulation.

A. Simulations of Message Transmissions

As mentioned before, the primary features of the communication network in the smart grid is two-fold: 1) varied multicast groups based on different applications; 2) time-constrained message deliveries [11]. In addition, since our objective for the co-simulation framework is to describe the complicated network behaviors in a statistical manner, we may not care about transmission details in the network, like channel interferences, routing protocols and so on. Therefore, we give up commonly used network simulators, such as NS2 and OMNeT++, but resort to NetworkX [20] towards an abstractive description of the communication network. The NetworkX is a python language software package for the creation, manipulation, and study of the structure and dynamics of complex networks, by using which, we are able to focus more on the topology changes of the network.

As shown in Algorithm. 1, we firstly generate the communication network topology through the degree distribution of the communication nodes[2], which is from the theory of the *contact network model* [21], a popular mathematical tool in the complex network study. As mentioned before, the

[2]The degree of a node in a network is the number of connections it has to other nodes, whereas the degree distribution is the probability distribution of these degrees over the whole network.

Algorithm 1 Algorithm of Alarm Message Propagations

Initialization:

Set z: node_degree_sequence; $t = 0$;
G: alarm_messg_multicast_topology is generated by z;
T_d: delay deadline of message propagations;
$E = (dt, node, \text{“}alarm\text{”})$: an alarm propagation event;
p: successful transmission probability;

Iteration:

randomly select the first alarm node $ASource$ from G;
$ASource \rightarrow E = (dt, ASource, \text{“}alarm\text{”})$;
$E \rightarrow EList$: push E into a event list $EList$;
while $t < T_d$ **do**
  $EList$ pop E;
  for all n in $E.node.multicast\_neighbors$ **do**
    if n does not hold $E.\text{“}alarm\text{”}$ **then**
      $E.node \rightarrow n$ *with* p
      if $Success$ **then**
        $n \rightarrow E = (dt, n, \text{“}alarm\text{”})$;
        $E \rightarrow EList$;
      end if
    end if
  end for
end while

Output:

Set of nodes with “alarm” S_{alarm};
Set of nodes with overdue “alarm” $S_{overdue}$;
Set of nodes with unsuccessful transmissions $S_{untrans}$;

Algorithm 2 Algorithm of Power Error Propagations

Initialization:

Set S_{alarm}: nodes with “alarm”; $ASource$: fault node;
$S_{overdue}$: nodes with overdue “alarm”;
$S_{untrans}$: nodes with unsuccessful transmissions;
$RCase$: test case used in simulation;
$EList$: an event list for power network errors;

Iteration:

$RCase = RCase - ASource$;
$Case_{normal}$ = re-run power flow ($RCase$);
if $S_{untrans}! = \{\phi\}$ **then**
  Fix node values of $S_{untrans}$ in $RCase$;
  $Case_{fail}$ = re-run power flow ($RCase$);
  for all $PowerFlow$ in $Case_{fail}$ **do**
    if $PowerFlow > RCase.maxflow$ **then**
      $S_{untrans}.node \rightarrow E = (S_{untrans}.node, \text{“}error\text{”})$
      $E \rightarrow EList$;
    end if
  end for
end if
if $EList == \{\phi\}$ **then**
  Simulation Ends;
else
  transfer $EList$ to Algorithm. 1;
end if

Output:

Final Power Network Status $Case_{normal}$;
Iteration Round I;

communication network topology is application-specific, that means that, communication topologies can follow different degree distributions for different applications, such as the uniform distribution and the power law distribution. In terms of the network size, it is determined by the IEEE test system [22], [23], which will be illustrated later in the power network simulation. With the degree distribution, as well as the total node number, we are able to derive the network topology.

In the generated network topology, we then randomly select a node as the source of the “alarm” message, which also entails the first fault device in the power network. The follow-up process is iterative to determine the node set with “alarm” messages before the transmission deadline. Whether a node is holding the “alarm” message is subject to the distribution of the successful transmission rate within the timing requirement, which follows a normal distribution regarding experimental results of our previous work [15].

As a result, we establish a NetworkX based component to emulate message propagations in the communication network. In what follows, we will apply results of the communication simulation to start the simulation of the power network.

B. Simulations of Electricity Deliveries

The simulation of the power network generally focuses on operations of electrical power system, including long-term power planning and short-term operational simulations. Accordingly, many critical elements of power systems are involved in the power system simulation based on different abstract levels, such as power flow study, short circuit analysis, transient stability, and optimal generator dispatching [24].

Since our objective is to study the performance affects of the communication network on the power network, we choose the power flow study as a preliminary tool to analyze the power system in the normal steady-state operation. As a relatively easy tool, the power flow study is prone to help us obtain some intuitive parameters, like the real power. There are various simulation tools available for the power flow simulation. To map with our communication part, we here adopt PYPower [23] for our power network simulation. PYPOWER is a direct python translation of MATPOWER [22] that is widely recognized as the most popular power flow analysis tool.

Algorithm. 2 illustrates our power network simulation. In the normal case, namely, no multicast transmission fails in the communication network, the fault node (either a bus, or a generator, or a transmission line) will be firstly removed from the original IEEE test case towards a post-fault topology, and then re-run the power flow calculation to achieve a new steady state of the test case. However, in the case that transmission failures exist, as the power flow calculation depends on the synergistic adjustments of generators, loads and transmission lines, all nodes failed to receive the alarm messages will be recognized to miss critical information of power adjustments. Accordingly, power parameters on these nodes will be kept without any changes. As a result, differences ensues between power flow calculations in the normal case and that in the

TABLE I
SUMMARY OF THE POWER TOPOLOGY IN IEEE TEST CASES.

Case Name	Bus	Generator	Branch	Total
9-Bus Case	9	3	9	21
14-Bus Case	14	5	20	39
30-Bus Case	30	6	41	77
118-Bus Case	118	54	186	358
300-Bus Case	300	69	411	780

transmission failed case. With these differences, we are able to determine *whether any nodes in the power network are secondary broken due to the failed message deliveries*[3]. If so, the corresponding secondary broken nodes will be pushed back to the event list as new fault sources to trigger another round of alarm message propagations. The iteration between the power network and the communication network will finish under two conditions, either some round of alarm message propagation is completed with no failure, or all critical nodes in the power network are broken, e.g., all generators loss power, all buses are broken, or all loads are shed.

Therefore, we establish a co-simulation framework to replay interesting interdependent behaviors between the communication and the power network. In what follows, we intend to leverage IEEE test system to investigate the affect of the coupled network architecture on the system reliability.

IV. PERFORMANCE RESULTS

In this section, we will take series of IEEE test cases [22], [23] as the topology of the power network to evaluate interdependent system behaviors between the communication network and the power network. Firstly, we present parameters used in the simulation. Then, two critical metrics are measured in our Networkx-PYPOWER co-simulation framework, including the ratio of failed alarm message transmission and the complementary cumulative distribution of the number of secondary fault nodes in the power network. Based on two metrics, we discuss insights implied in the experimental results for the communication network planning in the smart grid.

A. Experimental Setup

As mentioned before, the topology of the power network in our simulation follows the classical IEEE test case. In terms of the communication network, we assume that each power components in the test case have an IED attached with it. With these IEDs, we derive the network topology through aforementioned node degree distributions. The size of the corresponding communication networks is matched with IEEE test cases as shown in Tab. I.

Besides the size of the communication network, we use a power law distribution (with $exponent = 2.0$) to simulate the number of a node neighbor regarding the experimental results presented in [21]. Also, we leverage experimental results illustrated in [15] to assume the message transmission

[3]Note that, we here adopt 10 times of the rated power as the maximum value a device can bear. If the real power is 10 times larger than device's rated power, we will denote the device as damaged.

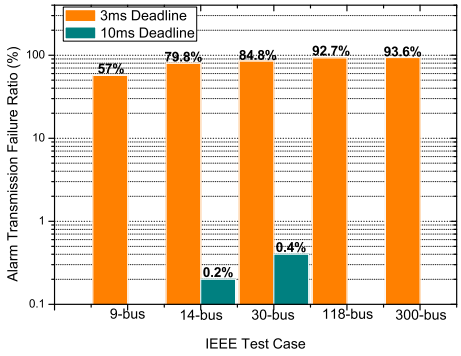

Fig. 4. The Ratio of Failed Alarm Message Transmissions in Different IEEE Power Test Cases.

delay to follow a normal distribution (with $\mu = 0.701ms$ and $\sigma = 0.18$)[4]. In terms of parameters used in the power network, we currently adopt the DC power flow calculation to study the power flow changes in the test cases.

B. Performance Results

The primary question we want to justify through the simulation is *how often communication failures will happen during the multicast alarm message transmissions in the required timing requirements*. The frequency of communication failures determines, *how possible the domino affect shown in Fig. 3 will appear*. We start from *one* power device fault to trigger alarm message transmissions in the communication network. Fig. 4 shows the ratio of trials, in which failed transmissions will happen in different test cases regarding two timing requirements, 3ms and 10ms, both which are critical timing requirements for teleprotection-related applications [11].

Through Fig. 4, we can see that, the ratio of the failed alarm message transmission exhibits significant differences in two delay requirements. When using 3ms as the delay threshold, even in the smallest network, 9-Bus case, transmission failures occur in 57% trails. The ratio keeps rising along with the increase of the network size, even up to 93.6% in the 300-bus case. Adversely, when 10ms delay requirements are adopted, the failed alarm transmission almost disappear in all cases. Thus, we can conclude that, the transmission failure should be considered for sure when planning communication networks for emergent transmissions with rigorous timing requirements. To reduce the possibility of the failed communication, we can choose more reliable communication technologies, like Ethernet, to replace the unreliable wireless links, thus saving timing costs of message deliveries. Also, the size of the multicast group ought to be fine-grained planned to match the timing requirement perfectly.

Furthermore, if the transmission failure is inevitable, the following question is *how many power nodes will be secondary damaged to raise the second round of alarm message transmissions*. Fig. 5 shows the complementary cumulative distribution of the number of the fault power nodes that are

[4]The μ and σ is from tests using one-hop 802.11g WiFi network.

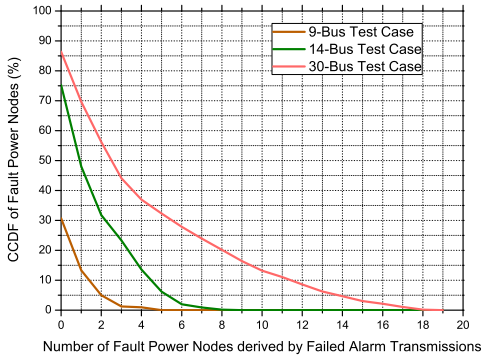

Fig. 5. Distributions of Secondary Fault Nodes in Power Networks.

results from the failed message transmissions. In 9-bus case, although the failed message transmission exists with a higher probability, there are still 70% trails, in which no fault power nodes are derived. In the worst case of the 9-bus system, 5 nodes may be secondary damaged, but with a low probability less than 0.2%. However, the situation becomes worse along with the network size increases. The number of the cascading fault node may attain to 9 in the 14-bus system, and even 19 in the 30-bus system. Even in the moderate case, the probability that at least 2 power nodes are derived from the communication failure is close to 50% in the 14-bus system, and close to 70% in the 30-bus system.

Therefore, we can summarize that, from Fig. 4 and Fig. 5, despite that the possibility of failed message transmissions is very low, the consequence is catastrophic, especially in a larger power network. That is, one power device failure will trigger network-wide traffics towards synergistic device actions. Once some nodes miss the alarm, at most 4 power nodes will be damaged due to the failed message transmission in the 9-bus system, at most 8 nodes in the 14-bus system, and at most 19 nodes in the 30-bus system.

V. Conclusion

In this paper, we first reviewed the unique system architecture of the smart grid, which is composed of two coupled, yet interdependent networks, including a communication network and a power network. With the system architecture, we analyze interactions of the two coupled networks in a fault happening scenario. Through the analysis, we claim an iterative fault propagation process that may superpose the time-critical transmission fault over the original power fault to enlarge the fault size and to result in more power devices damaged. To testify the potential domino affect in the coupled networks, we propose a co-simulation framework to integrate the communication network simulation with the power-flow based power network simulation. By using the co-simulation framework, we deploy two experiments to evaluate the probability of the message transmission failures in two typical timing requirements, and the number of secondary damaged power nodes derived by the failed communication transmissions. Our results reveal that, delay thresholds should be determined carefully to avoid a high probability of the transmission failure, as the consequence of transmission failures are catastrophic with many power nodes secondary affected. The results presented in this paper will benefit both the power engineer and the communication engineer when planning the communication facilities in the smart grid.

References

[1] 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*, pp. 1–145, Jan. 2010.
[2] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, August 2011.
[3] S. Buldyrev, R. Parshani, G. Paul, H. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," in *Nature*, 2010.
[4] B. Falahati and Y. Fu, "A Study on Interdependencies of Cyber-Physical Power Networks in Smart Grid Applications," in *The Conference on Innovative Smart Grid Technologies (ISGT2012)*, January 2012.
[5] J. Shao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "Cascade of failures in coupled network systems with multiple support-denpendence relations," *Phys. Rev. E*, vol. 83, p. 036116, Mar. 2011.
[6] J. Gao, S. V. Buldyrev, H. E. Stanley, and S. Havlin, "Networks formed from interdependent networks," *Nature Physics*, vol. 8, pp. 40–48, Jan. 2012.
[7] Grass Valley, "Trinix - digital video router back-up power supplies," http://www.grassvalley.com/docs/Manuals/routers/trinix_nxt/071-8443-02.pdf 2009.
[8] Cisco, "Connecting cables to cisco 3800 series routers," http://www.cisco.com/en/US/docs/routers/access/3800/hardware/installation/guide/38cable.html#wp1008449 2009.
[9] A. J. Wood and B. F. Wollenberg, "Power generation, operation and control," *John Wiley and Sons, 2nd edition*.
[10] A. Huang, M. Crow, G. Heydt, J. Zheng, and S. Dale, "The future renewable electric energy delivery and management (freedm) system: The energy internet," *Proceedings of the IEEE*, 2011.
[11] X. Lu, W. Wang, and J. Ma, "An empirical study of communication infrastructures towards the smart grid: Design, implementation and evaluationnergy internet," *IEEE Transaction on Smart Grid*, to appear.
[12] R. Lasseter and P. Paigi, "Microgrid: a conceptual solution," in *Power Electronics Specialists Conference, 2004. PESC 04. 2004 IEEE 35th Annual*, vol. 6, june 2004, pp. 4285 – 4290 Vol.6.
[13] X. Lu, Z. Lu, W. Wang, and J. Ma, "On Network Performance Evaluation toward the Smart Grid: A Case Study of DNP3 over TCP/IP," in *Proc. of IEEE Globecom'11*, December 2011.
[14] X. Lu, W. Wang, Z. Lu, and J. Ma, "Reliable and Secure Communication Platforms of FREEDM Systems in Smart Grid," in *Proc. of IEEE Mobicom'11 (Demo Session)*, September 2011.
[15] X. Lu, W. Wang, and J. Ma, "Authentication and integrity in the smart grid: An empirical study in substation automation systems," *International Journal of Distributed Sensor Networks*, April 2012.
[16] IEC, "IEC 61850 communication networks and systems in substations," 2003.
[17] G. G. Karady and X. Liu, "Fault management and protection of freedm systems," in *Power and Energy Society General Meeting, 2010 IEEE*, July 2010.
[18] X. Lu, W. Wang, Z. Lu, and J. Ma, "From Security to Vulnerability: Data Authentication Undermines Message Delivery in Smart Grid," in *Proc. of IEEE Milcom'11*, November 2011.
[19] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. of IEEE Conference on Computer Communications (INFOCOM' 11)*, Apr. 2011.
[20] "Networkx," http://www.networkx.lanl.gov.
[21] M. E. J. Newman, S. H. Strogatz, and D. J. Watts, "Random graphs with arbitrary degree distributions and their applications," *Phys. Rev. E*, vol. 64, Jul 2001.
[22] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *Power Systems, IEEE Transactions on*, Feb. 2011.
[23] "Pypower," http://www.pypower.org.
[24] J. J. Grainger and W. D. Stevenson, "Power system analysis," *McGraw-Hill Science*, January 1994.