Effects of Cyber Coupling on Cascading Failures in Power Systems

Xi Zhang, Dong Liu, Choujun Zhan, and Chi K. Tse, *Fellow, IEEE*

***Abstract*—In this paper, we propose a model to investigate the cascading failures in the coupled system (smart grid) that comprises a power grid and a coupling cyber network. In this model, we take into consideration the effects of power overloading, contagion and interdependence between power grids and cyber networks on failure propagations in the coupled system, and then use a stochastic method to generate the time intervals between failures, thus producing the dynamic profile of the cascading failures caused by the attack of cyber malwares. We study several coupled systems generated by coupling the UIUC 150 Bus System with cyber networks of different structures and coupling patterns. Simulation results show that the dynamic profile of the cascading failures in a coupled system displays a "staircase-like" pattern which can be interpreted as a combined feature of the typical step propagation profile triggered repeatedly by cyber attacks due to network coupling. Results also show that cyber coupling can intensify both the extent and rapidity of power blackouts. Moreover, the cyber network structure and the coupling patterns affect the propagation of the cascading failures in smart grids. Scale-free cyber networks promote failure spreading, and the higher average cyber node degree also intensifies the spreading. Coupling power nodes with high-degree cyber nodes accelerates the failure propagation compared to random or low-degree couplings.**

***Index Terms*—Interdependent infrastructures, cascading failure, power system, cyber attack.**

I. Introduction

SMART grids are defined as electrical networks with integration of information and communication technologies (ICT) to deliver electric power to the final consumers more efficiently and securely [1]. A smart grid is a typical cyber-physical system (CPS) [2], where the physical part is the power apparatus in the power grid and the cyber part is for state monitoring, communications, and control of the physical network. Coupling with cyber networks can make smart grids more efficient and intelligent, at the same time it may bring new challenges by making power systems more vulnerable to attacks from cyber networks [3]–[5].

As computers are in control of critical devices in today's power systems at every level [6], attacking power systems via spreading malware in computer networks may cause severe damages or even catastrophic consequences. The Aurora Generator Test conducted by Idaho National Laboratory demonstrated how a generator can be physically destroyed by a piece of codes [7]. Cyber malware can attack multiple points of the physical network and may jeopardize the CPS [6]. The latest demonstration of a severe blackout caused by cyber attacks took place on December 23, 2015 in Ukraine [8], which was planted by a computer malware (called BlackEnergy) that penetrated the computer network connected to the Ukrainian power system through an infected file downloaded by the operator. BlackEnergy silently infected workstations in the cyber network for several months, and then attacked the system by disconnecting breakers of several substations, making monitoring stations go blind and blocking the call centers. Finally, 80,000 customers were deprived of power for more than six hours.

In the past two decades, numerous studies were devoted to the cascading failure analysis in power systems, focusing mainly on the physical network. Having witnessed the threats from cyber coupled attacks, power engineers and researchers are becoming more aware of the importance of understanding the behavior of cyber coupled power systems. Future smart grids will certainly be heavily dependent on safe and efficient operation of coupled power apparatus and communication networks. With this new motivation, researchers have recently diverted attention to the smart grids' vulnerability assessment and mitigation methods to cyber attacks [9]–[12].

Abstracting the substations as nodes and the transmission lines as edges, the power physical layer can be modeled as a network. Correspondingly, the cyber layer can also be represented as a complex network, in which computers are nodes and the cyber connections are edges. Considering the interdependence of these two networks (i.e., power nodes provide power to the nodes in cyber layer, and the cyber nodes control the operation of power nodes), the behavior of smart grids can be studied from a perspective of interdependent complex networks [13]–[15].

Buldyrev *et al.* in 2010 [16] studied failures in interdependent networks with percolation theory and concluded that networks with a broader degree distribution were more vulnerable. In percolation theory, all nodes in the network are deleted with a probability, which can fragment the network. The nodes that belong to a giant cluster are assumed to be able to function well, while the nodes in the remaining small clusters become malfunctioned. Cai *et al.* in 2016 [17] analyzed the cascading failures in power systems considering the interaction between power grids and communication networks. Failure of a power element is determined by the time when

Manuscript received October 15, 2016; revised January and February 2017. This work is supported by Hong Kong Research Grants Council GRF Project PolyU 5258/13E.

X. Zhang, D. Liu and C.K. Tse are with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hunghom, Hong Kong. (Email: xi.r.zhang@connect.polyu.hk, adam.d.liu@connect.polyu.hk, encktse@polyu.edu.hk)

C. Zhan is with the Department of Electronics Communication and Software Engineering, Nanfang College of Sun Yat-sen University, Guangzhou 510900, China. (Email: zchoujun2@gmail.com)

Digital Object Identifier 00.0000/JETCAS.2017.0000000000

it is overloaded and the duration of data dispatching in the communication network. Rahnamay-Naeini *et al.* in 2016 [18] modeled the number of failures in a power grid and the number of failures in a communication network as two interdependent time series. Stochastic methods are adopted to analyze the dynamical profiles of these time series. It has been concluded in Rahnamay-Naeini *et al.*'s study that interdependence can make the individually reliable systems behave unreliably as a whole. Although these prior studies focused on interdependent networks composed by the power network and the cyber network, they fall short of taking into consideration the influence of computer malware on the operation of power systems. In the Ukrainian case, for instance, the malware infection in the cyber network plays an important role in the cascading failure propagation in smart grids. Our previous work [19] showed that the mechanism of failure propagation in a power grid is very different from that of malware spreading in an individual cyber network [20]. However, for the smart grid where the physical layer and the cyber layer are highly mutual dependent, the cascading failures can be highly affected by the dynamics of computer malware spreading. Thus, the dynamic property of malware spreading should be considered in cascading failures in the case of smart grids.

In this paper, we investigate the effects of cyber coupling on cascading failures in smart power grids. First, the mechanism of failure spreading in the power system (due to power overloading) and that in the cyber network (due to malware contagion) are considered in the model, with emphasis on the interdependence of these two networks. Then, based on the corresponding mechanisms, we combine the deterministic circuit-based model and a stochastic method to describe the failure processes of the two kinds of nodes in the coupled system in Section II. Then, we introduce an algorithm to simulate the cascading failures in the coupled system in Section III. We simulate several coupled systems and summarize key findings in Section IV. The coupled systems are generated by coupling the UIUC 150 Bus System with cyber networks of various structures and coupling patterns. Simulation results show that the failure propagation pattern in a coupled system displays characteristics of both the power network and the cyber network, and that cyber coupling can cause more severe damages to the power system. The cyber network structure as well as the coupling pattern play crucial roles in the propagation of the cascading failures in smart grids. Scale-free cyber networks promote the failure spreading in the coupled system, and a higher average node degree of the cyber network intensifies the spreading. Moreover, coupling of power nodes with high-degree cyber nodes makes failure propagate faster compared to coupling randomly or with low-degree nodes.

II. Model Description

In this paper, we consider a smart grid composed of a set of power apparatus and its controlling network. The controlling network refers to the specific computer network for controlling power systems, which is normally isolated from the wide area network we use in other applications. In practice, firewalls and other security measures should be designed and applied in these important networks. For simplicity, we consider a coupled system A–B which is composed of two interdependent networks A and B, as shown in Fig. 1. Network A is the power grid, where solid rectangular nodes in Fig. 1 represent electrical buses in A and solid arcs represent transmission lines. Network B is the cyber network, where white circular nodes represent computers in the cyber network and dashed joining arcs represent the connections among the cyber nodes. Clearly, nodes in A and nodes in B are interdependent. Precisely, the cyber nodes control the operation of power nodes, while the power nodes provide power to the cyber nodes. The interdependent relationships are depicted by the horizontal lines in Fig. 1. In this paper, we consider one-to-one coupling relation between the nodes in A and the nodes in B, i.e., $A_i \leftrightarrow B_i$. Each pair of coupled nodes (A_i and B_i) are called a *node pair* in the coupled system A–B. For the sake of maintaining generality, we also consider nodes without corresponding coupling nodes in the other network. For these nodes, there are no coupling effects. In Fig. 1, there are p power nodes, q cyber nodes and m *node pairs*, where $p \geq m$ and $q \geq m$. Usually the number of nodes in the cyber network is far bigger than that of the power network, i.e., $q \gg p$.

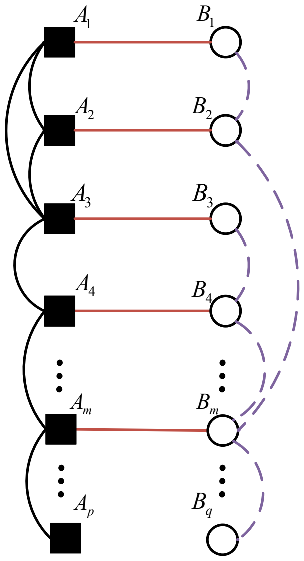


Fig. 1. Coupled network consisting of a power network A and a cyber network B. Solid rectangles represent electrical buses and solid arcs represent transmission lines in A. White circles represent computers in the cyber network and dashed arcs represent connections among the cyber nodes in B. Horizontal lines represent interdependence between nodes in A and nodes in B.

In this paper, we study the cascading failures in the coupled system A–B, which is initiated by attacks of computer malwares. The cascading failure propagation in A–B can be viewed as a sequence of state transitions of the nodes in the coupled system. In the following subsections, we will define the states of nodes and describe their corresponding state transitions.

A. Failure Mechanism of Power Elements

In this section, we introduce the mechanism of the electrical elements' failures. Previous works have analyzed cascading

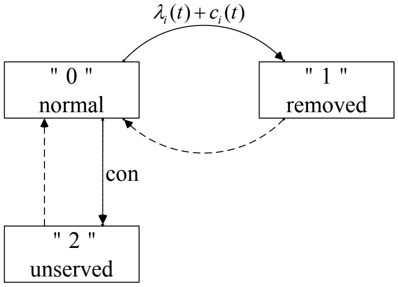


Fig. 2. State transition diagram of a node in power network A. Transitions between state 0 and 2 are deterministic transitions, and those between 0 and 1 are stochastic transitions.

failures in individual power systems. Data fitting methods have been applied to study the failure propagation profiles in power systems in refs. [21], [22], regardless of the physical failure cascade mechanism in the network. Considering the effects of power flow distribution in the failure propagation, several models have been proposed to simulate the cascading failure propagations in power systems, which can be classified under two categories: *deterministic* models and *stochastic* models. In deterministic models [19], [23], in each round of the cascading failure process, the power flow distribution in the network is computed, and overloaded electrical elements are removed at the same time. To show the dynamic profile, Eppstein *et al.* [24] made the simple deterministic assumption that the duration for an overloaded element to be tripped is equal to Δt which is given by $\int_t^{t+\Delta t}(f_j(\tau) - \bar{f}_j)d\tau = \Delta o_j$, where f_j is the power flow of overloaded element j, $\bar{f}_j$ is the flow limit and Δo_j is a specific threshold of that element. Considering the high uncertainties and complexities in power systems, stochastic models are used to investigate cascading failures in power systems [26]–[28], but a mathematical formula that can describe the collective behavior of the power network has not been derived.

In modeling the failure cascading in a power grid in this paper, we first apply *deterministic* power flow analysis to derive the power flow information and the overloading conditions of the electrical elements. Then, we adopt a stochastic method to obtain the time durations between failures to simulate the failure propagations in the network.

Let s_{A_i} denote the state of a power node A_i. In our model, we consider three possible states for a power node, i.e., $s_{A_i} \in \{0, 1, 2\}$. Specifically, $s_{A_i} = 0$ is the normal state, which corresponds to node A_i being connected and operating normally in the power network; $s_{A_i} = 1$ is the removed state, which corresponds to A_i being tripped by a circuit breaker and removed from the power network; and $s_{A_i} = 2$ is the unserved or "islanded" state, which corresponds to A_i being inaccessible to power sources due to the removals of other failed elements in A. When A_i is in state 1 or 2, it is deprived of power. Possible state transitions of A_i are shown in Fig. 2.

Depending on the nature of the transitions, they are either deterministic transitions or stochastic transitions, as shown in Fig. 2. The tripping (removal) of some elements in A can fragment the power network into several disconnected sub-networks. When a sub-network containing no power source is created, a condition "con" is said to be reached for all nodes in the sub-network. Under this condition, nodes in the sub-network change their states from 0 to 2. This state transition, namely $s_{Ai} = 0 \xrightarrow{\text{con}} s_{Ai} = 2$, is deterministic. Moreover, this state transition is caused by and always accompanying the state transition ($0 \to 1$) of another element in A, and thus the transition time for this type of state transitions is not considered.

On the other hand, the time at which a stochastic state transition takes place is an important consideration that would affect the dynamic profile of the cascading failure propagation. Node A_i (in state 0) is tripped by its protective equipment with a certain probability value when A_i is overloaded or when its coupled node B_i is infected by a computer malware that can attack the power network by switching off circuit breakers of A_i. The stochastic state transition of node A_i from state 0 to state 1 is represented by a *state transition channel* T_1, and is represented as:

$$T_1 : s_{Ai} = 0 \to s_{Ai} = 1. \tag{1}$$

When node A_i has a coupled node B_i which works normally or does not have a coupled node in network B, the state transition $s_{Ai} = 0 \to s_{Ai} = 1$ is only caused by overloading. In much of the prior work on modeling the switching actions of the relays using Markov models [26] [27], transitions are determined by power loading conditions and elements' capacities. In real-time operation, as pointed out by Sun *et al.* [29], an electrical component's failure rate is not constant but varies with loading conditions, and that a component will experience more failures under heavy loading conditions. In order to incorporate these characteristics in our model, we describe the state transition $s_{Ai} = 0 \xrightarrow{\lambda_i(t)} s_{Ai} = 1$ as a stochastic process and define the tripping rate λ_i as

$$\lambda_i(t) = \begin{cases} a_i\left(\dfrac{L_i(t) - C_i}{C_i}\right), & \text{if } L_i(t) > C_i \\ 0, & \text{if } L_i(t) \le C_i \end{cases} \tag{2}$$

where $L_i(t)$ is the power loading of component i , C_i is the capacity of that component, and a_i is the basic unit rate (trippings per second). Using (2), the power flow analysis can be applied to derive $\lambda_i(t)$. In this paper, we adopt the method introduced in [19] to compute the power flows in the power system, assuming that the power system will reach a new steady state after an element fails. In this paper, we do not consider stability issues that have been studied in [30], [31]. Thus, when A_i is in state 0, and on the condition that its coupling node B_i is working normally or it has no coupling nodes in network B, the probability that A_i transits from state 0 to 1 in an infinitesimal time interval dt can be written as

$$T_1 : P[s_{Ai}(t + dt) = 1 \mid s_{Ai}(t) = 0] = \lambda_i(t)dt. \tag{3}$$

When A_i has a coupling node B_i in network B and B_i is infected by a computer malware, A_i (in state 0) will have an extra chance to be removed from system due to the action of malware. Thus, we assume that the malware will add an additional rate $c_i(t)$ to the state transition rate λ_i. Thus, the probability that A_i transits from state 0 to 1 in an infinitesimal

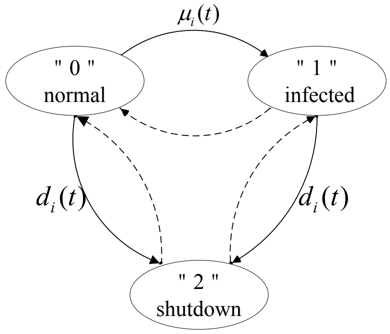


Fig. 3. State transition diagram of a node in the cyber network B.

time interval dt when B_i is infected by computer malware can be written as

$$T_1 : P[s_{Ai}(t+dt) = 1 \mid s_{Ai}(t) = 0] = (\lambda_i(t) + c_i(t))dt, \tag{4}$$

where $c_i(t)$ represents the dependency of power node A_i on cyber node B_i.

State 1 and state 2 are fundamentally different states even though both correspond to an unserved node. For state 1, the power node is removed due to it being tripped by the protective relay upon power overloading. We use a stochastic method to describe this process. However, for state 2, the power node has no access (finds no path) to power sources due to the tripping of other elements in the network. Though unserved, it is not tripped and is still well connected. We use a deterministic method to describe this process, and it depends on the tripping of other elements in the network. From the network's point of view, an element in state 1 is an open-circuit, changing the topology of the network, whereas an element in state 2 has no impact on the network topology.

In a fast cascading failure process, we do not consider repair and anti-malware actions. Thus, the corresponding transition rates are set as 0, i.e., dashed arrows in Fig. 2 are neglected.

B. Failure Mechanism of Cyber Nodes

Let s_{B_i} denote the state of node B_i. We consider three different states for a cyber node B_i, namely states 0, 1 and 2. Specifically, $s_{B_i} = 0$ is the normal state, in which B_i is working normally in the cyber network; $s_{B_i} = 1$ is the state of being infected by a computer malware; and $s_{B_i} = 2$ is the shutdown state corresponding to node B_i being shut down due to power outage. The difference between state 1 and state 2 is that when a computer is infected (in state 1), it is able to infect its neighboring nodes, whereas a shutdown computer (in state 2) is completely removed from the cyber network and does not infect others. Fig. 3 shows the state transition diagram of cyber node B_i. All state transitions of B_i are stochastic transitions. Details of the transition process are as follows.

When node B_i is in state 0, it can be infected by a computer malware through connection with an infected neighbor. The malware diffusion can be modeled by a stochastic process [20]. Here, we use describe B_i's state transition as $s_{B_i} = 0 \xrightarrow{\mu_i} s_{B_i} = 1$, and refer to it as state transition channel T_2:

$$T_2 : s_{B_i} = 0 \xrightarrow{\mu_i} s_{B_i} = 1. \tag{5}$$

where μ_i is the rate of infection of node B_i and is defined as

$$\mu_i(t) = \sum_{j \in \Omega_{Bi}} \beta_{ij}, \tag{6}$$

where Ω_{B_i} is the set of all infected neighbors of node B_i and β_{ij} is the rate at which infected node B_j ($s_{B_j} = 1$) infects its neighbor B_i which is in state 0. For an infinitesimal time interval dt, the probability that a state transition occurs through T_2 can be written as

$$T_2 : P[s_{B_i}(t+dt) = 1 \mid s_{Bi}(t) = 0] = \mu_i(t)dt. \tag{7}$$

When node B_i has a corresponding coupled power node A_i and $s_{A_i} \in \{1,2\}$, it can no longer provide power to its cyber node B_i, causing B_i to transit to state 2 (shutdown) due to power outage. In practice, usually there exists backup power for computers that perform crucial functions in controlling the power grid. Considering the limited supporting time of the backup power units, in our model, we use stochastic transitions to describe the state transitions for node A_i when $s_{A_i} \in \{1,2\}$. Specific details are as follows.

When $s_{B_i} = 0$ and $s_{A_i} \in \{1,2\}$, apart from state transition channel T_2, another state transition channel T_3 exists:

$$T_3 : s_{B_i} = 0 \xrightarrow{d_i} s_{B_i} = 2, \tag{8}$$

where $d_i(t)$ is the state transition rate which is determined by the dependence of node B_i on its coupled power node A_i. In an infinitesimal time interval dt, the probability that a state transition occurs through T_3 can be written as

$$T_3 : P[s_{B_i}(t+dt) = 2 \mid s_{B_i}(t) = 0] = d_i(t)dt, \tag{9}$$

When $s_{B_i} = 1$ and $s_{A_i} \in \{1,2\}$, there is another state transition channel T_4:

$$T_4 : s_{B_i} = 1 \xrightarrow{d_i} s_{B_i} = 2. \tag{10}$$

In time interval dt, the probability that a state transition occurs through T_4 can be written as

$$T_4 : P[s_{B_i}(t+dt) = 2 \mid s_{B_i}(t) = 1] = d_i(t)dt. \tag{11}$$

Finally, as repair or anti-malware actions are not considered in a fast cascading failure process, the corresponding transition rates can be set to 0, i.e., dashed arrows in Fig. 3 are neglected.

III. Cascading Failures in Coupled Systems

The coupled system A–B contains p power nodes, q cyber nodes, and m node pairs in total. Let $S(t)$ denote the state of A–B, and $S(t) = [s_{A_1}, s_{A_2}, \cdots, s_{A_p}, s_{B_1}, s_{B_2}, \cdots, s_{B_q}]$. There can be 3^{p+q} possible states for A–B. The cascading failure process is the dynamic propagation profile of $S(t)$ as the system state transits in time among those 3^{p+q} different states.

A. State Transition of the Coupled Network

Suppose, at time t, the coupled network is in state $S(t) = N_S$ (N_S is one specific system state of the 3^{p+q} possible states), and there are u nodes that may undergo a state transition. Each node of these u nodes can undergo a deterministic or stochastic transition, depending on the current node state and

TABLE I

State transition channel list of the coupled system at time t given that $S(t) = N_S$. All the l nodes which may transit and their corresponding transition rates are listed.

Possible transition channel	$T^{(1)}$	$T^{(2)}$	$T^{(3)}$	...	$T^{(n)}$
Transition rate	r_1	r_2	r_3	...	r_n

the transition rule. For a deterministic transition, the transition rule is triggered when condition "con" is met, while for a stochastic transition, the transition rule is described by a transition rate, as shown in Figs. 2 and 3. At time t, there are l ($l \leq u$) nodes that will undergo a stochastic transition, and each one will transit through a transition channel selected from T_1, T_2, T_3, T_4. For instance, if cyber node B_i is in state 0 (i.e., $s_{B_i} = 0$) at time t and is connected to an infected neighbor, and at the same time its coupled power node is removed or unserved, then node B_i will have two state transition channels, namely, T_2 and T_3. Thus, the total number of transition channels (say n) can be larger than l. In our algorithm, we first identify condition "con", and transit all power nodes meeting "con" to state 2 instantly. Then, all possible stochastic state transition channels of the coupled system is listed in a *state transition channel list*, as shown in Table I, where channel $T^{(i)} \in \{T_1, T_2, T_3, T_4\}$. Any node's state transition through any one of the n transition channels will lead to a state transition of the coupled network, i.e., change in $S(t)$.

The cascading failure process can be viewed as a sequence of state transitions. We only allow one element state transition at a time. That is, at most one state transition channel is chosen at a time. See Appendix for a rigorous argument. In order to simulate the dynamic propagation of $S(t)$, we need to

1) find the time at which a state transition occurs; and
2) identify the corresponding transition channel through which the transition occurs.

The following subsection explains the detailed process of finding transition time and identifying the transition channel.

B. Stochastic Transition Processes

Let $Q(\tau)$ denote the probability that no state transition occurs in time interval $(t, t+\tau)$, i.e., $Q(\tau) = P[S(t+\tau) = N_S \,|S(t) = N_S\,]$. Then, $Q(\tau + dt)$ can be written as

$$Q(\tau + dt) = P[S(t+\tau+dt) = N_S \,|S(t+\tau) = N_S\,]Q(\tau). \quad (12)$$

Thus, we have

$$P[S(t+\tau+dt) = N_S \,|S(t+\tau) = N_S\,] = (1 - r^* dt), \quad (13)$$

where $r^* = \sum_{i=1}^{n} r_i$. Note that equation (13) is only valid when dt is infinitesimally small (see Appendix). Substituting (13) into (12), we get

$$Q(\tau + dt) = Q(\tau)(1 - r^* dt). \quad (14)$$

Re-arranging (14), as $dt \to 0$ (i.e. dt is infinitesimal), we get

$$\lim_{dt \to 0} \frac{Q(\tau + dt) - Q(\tau)}{dt} = Q^{'}(\tau) = -r^* Q(\tau). \quad (15)$$

Thus, we can express $Q(\tau)$ as

$$Q^{'}(\tau) = -r^* Q(\tau).$$

Note that in equations (13) through (15), the above differential equation is derived by taking the limit $dt \to 0$ and is valid for any τ. Solving the above differential equation, we get

$$Q(\tau) = Q(0)e^{-r^*\tau}. \quad (16)$$

Since $Q(0) = P[S(t) = N_S \,|S(t) = N_S\,] = 1$, we can derive the expression of $Q(\tau)$ as

$$Q(\tau) = Q(0)e^{-r^*\tau} = e^{-r^*\tau}, \quad (17)$$

which is the general solution for $Q(\tau)$ and remains valid for all τ. Let $F(\tau)$ denote the probability that the next state transition occurs before time $t + \tau$. Then, we get

$$F(\tau) = 1 - Q(\tau) = 1 - e^{-r^*\tau}. \quad (18)$$

The probability density of τ can be found using equation (18) as

$$f(\tau) = r^* e^{-r^*\tau}. \quad (19)$$

From (18) and (19), we see that τ follows an exponential distribution. The state transition rate r^* of coupled system A–B is the sum of the transition rates of all the transition channels. As discussed in Section II, r^* includes the effects of overloading in the power network, malware spreading in the cyber network, and the interdependence between of two networks.

Suppose the next state transition occurs at time τ through transition channel T_k. To include the property of exponential distribution of τ and the characteristic that the transition channel with a higher rate will be more likely chosen, the following procedure is used to determine the next state transition.

Two random numbers z_1 and z_2 are uniformly and independently generated in $(0, 1)$. Then, τ is generated from the following equation :

$$\tau = F^{-1}(z_1) = \frac{1}{r^*}\ln(\frac{1}{1 - z_1}). \quad (20)$$

And k is selected based on the following equation:

$$\sum_{j=0}^{k-1} \frac{r_j}{r^*} \leqslant z_2 \leqslant \sum_{j=0}^{k} \frac{r_j}{r^*}. \quad (21)$$

The dynamics of $S(t)$ is a series of the state transitions introduced above beginning with an initial failure (malware injection) until all state transition channels are exhausted. Fig. 4 shows the flow chart used in simulating the cascading failures in the coupled system.

C. Simulation Flow Chart

- *Initialization:* The information of the coupled system A–B is set, including the network structure of A and B, and the coupling between the nodes in A and the nodes in B. In simulating the power failure propagation, the power flow calculation is necessary. Thus, for the power network, the admittance of the transmission lines, voltages of the

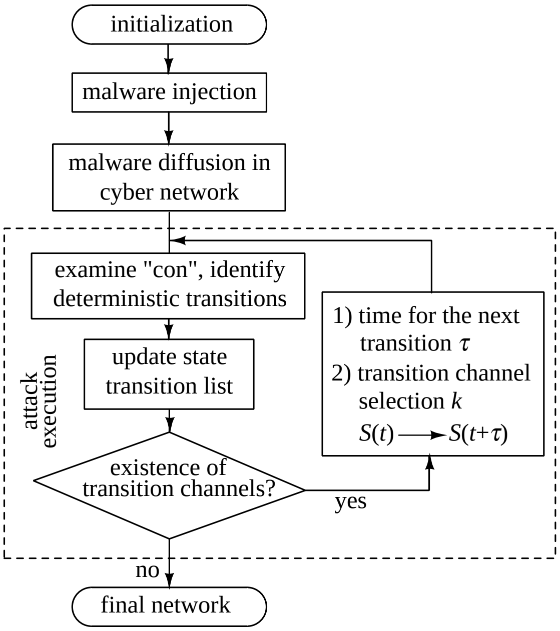

initialization
malware injection
malware diffusion in cyber network
attack execution
examine "con", identify deterministic transitions
update state transition list
existence of transition channels?
1) time for the next transition τ
2) transition channel selection k
S(t) → S(t+τ)
yes
no
final network

Fig. 4. Simulation flow chart for cascading failures in the coupled system.

generates, load demands of the consumers and winding ratios of transformers should be given.

- *Malware injection:* In this study, we assume the cascading failures are caused by cyber malware attacks. Thus, the initial trigger is the injection of a malware in the cyber network. The time of malware injection is set as 0.
- *Malware diffusion:* In the case of cyber attacks, the malware can be designed to spread silently and harmlessly in the cyber network for a period of time in order to get enough nodes infected. Here, we set t_d as the time period for the malware diffusion before attack is launched to the power network, and in this time period, only transition channels applied to the cyber network are relevant.
- *Attack execution:* After t_d, the malware will launch attack to the power system. All possible transition channels may be selected. Iteration then proceeds as follows.

  (a) The condition "con" will be checked against $S(t)$, and the power nodes meeting "con" are marked as state 2, i.e., the deterministic state transition occurs. This kind of state transitions occurs instantly.

  (b) Based on $S(t)$ and equations (3)-(11), we update the list of possible state transition channels. The list contains the rates contributed by all the failure spreading mechanisms in the coupled system, including power elements' failure due to power overloading based on equation (2) where the deterministic power flow analysis should be applied [19], cyber nodes' infection due to contagion based on equation (6), and the interdependencies between the two different networks.

  (c) If there is a state transition channel in the list, we use equations (20) and (21) to select the next state of $S(t)$ and return to step (a). If there is no more transition channel in the list, cascading failure ceases to propagate and the system is said to enter an absorbing state. We end the iteration and record the time as t_{final}.

IV. Simulation Results and Discussions

In this section, we perform simulation experiments with the proposed model to study the cascading failures in the coupled system and investigate the effects of cyber coupling on the failure propagation process. We specifically aim to identify the key factors and parameters that determine the extent and rapidity of power blackouts caused by cyber attacks. Test networks are generated by coupling the UIUC-150 Bus System [32] with cyber networks of different structures. The capacities of the generators, transformers and the transmission lines in the power network are set as 1.2 times of their respective current flows in normal operation. We also assume that the computer malware will execute attack once it infects a new cyber node, namely, $t_d = 0$. We introduce two essential metrics for characterizing the extent of the failure, namely, *percentage of failed power nodes* (PFPN) and *percentage of failed cyber nodes* (PFCN), which are defined as follows:

$$\text{PFPN}(t) = \frac{n_{\text{unserved}}(t) + n_{\text{removed}}(t)}{p}, \tag{22}$$

$$\text{PFCN}(t) = \frac{n_{\text{infected}}(t) + n_{\text{shutdown}}(t)}{q}, \tag{23}$$

where $n_{\text{unserved}}(t)$ and $n_{\text{removed}}(t)$ represent the number of power nodes in state 1 and 2 at time t, respectively. Similarly, $n_{\text{infected}}(t)$ and $n_{\text{shutdown}}(t)$ are the number of cyber nodes in state 1 and 2 at time t, respectively. Note that a large PFPN(t) (PFCN(t)) means that a large total area of disconnected fragments of the power grid (cyber network) are out of operation.

A. Failure Propagation Patterns in the Coupled System

First, we examine the failure propagation patterns in the power network, cyber network and the coupled system. We first study the case where the coupled cyber network has the same structure as the power grid. This allows a close examination of the failure spreading patterns on the power network and the cyber network due to the different spreading mechanisms. The parameters of the coupled network are set as follows:

- The cyber network and the power grid have the same size, i.e., $p = q = 150$;
- The failure rate in power system a_i is 0.21 min^{-1}, and the infection rate in the cyber network β_{ij} is 0.5 min^{-1};
- Interaction relationship between the two networks are $c_i(t)$ = 0.05 min^{-1} and $d_i(t)$ = 0.01 min^{-1}.

We obtain the values of a_i and β_{ij} through data fitting in this paper. For a_i, we get the value through setting the averaged t_{final} of 100 simulations in the UIUC 150 Bus system as 5 hours, based on the practical observation that the durations of several historical cascading failures were around 1 to 5 hours [33], [34]. For setting β_{ij} in the cyber network, we need to clarify that different malwares (viruses) can have very distinct infection rates. In this paper we adopt the values used in a

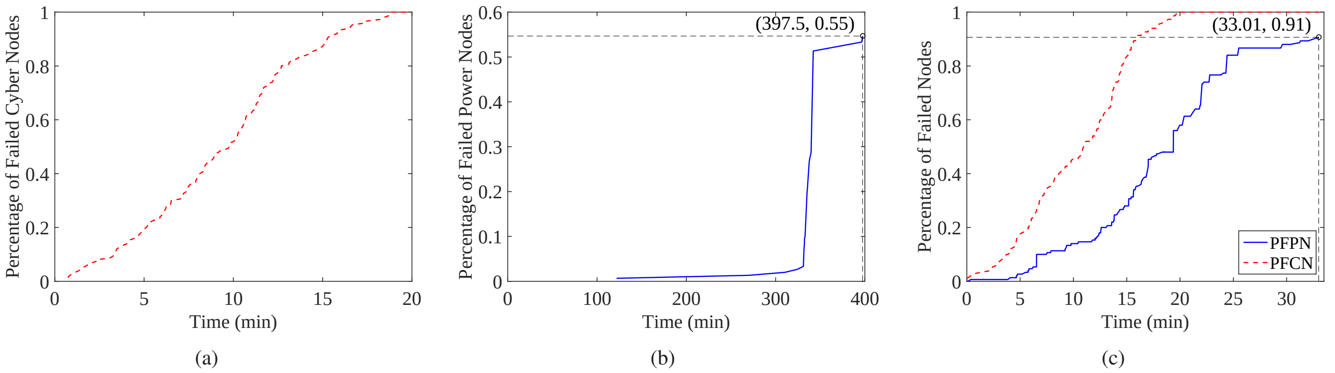


Fig. 5. Failure propagation in (a) cyber network showing smooth growth pattern; (b) uncoupled power grid showing "step jump" pattern; (c) coupled system.

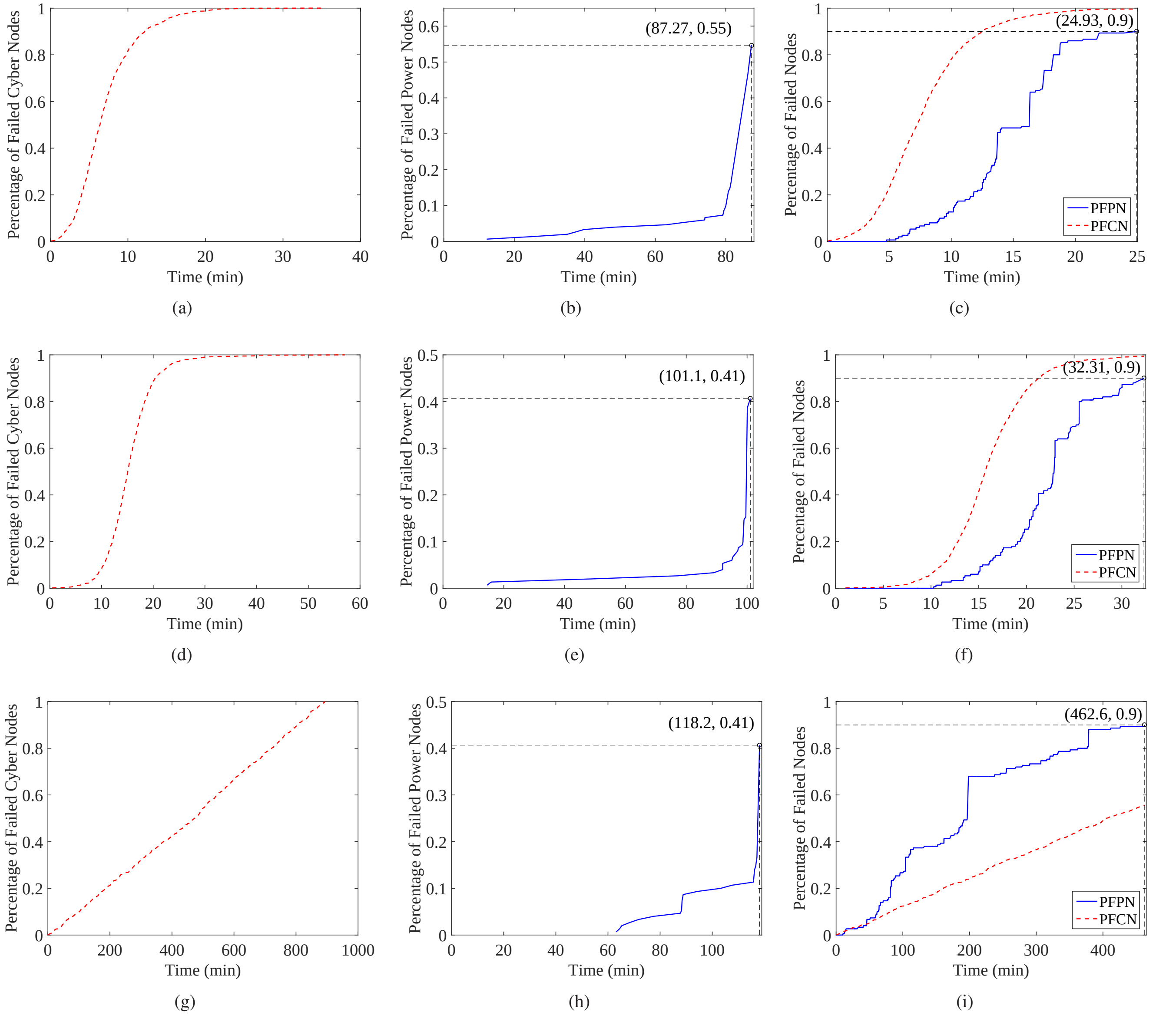


Fig. 6. Failure propagation patterns. (a), (d), (g): malware spreading in cyber network with scale-free, random and regular structure, respectively; (b), (e), (h): power node failure propagation in (uncoupled) power grid; (c), (f), (i): failure cascading in the coupled system, with scale-free, random, regular cyber network, all showing "multiple-step staircase" pattern.

TABLE II
COMPARISON ON SEVERITY OF CASCADING FAILURES BETWEEN THE ISOLATED POWER GRID AND THE COUPLED SYSTEM IN TERMS OF CASCADING FAILURE EXTENT DENOTED BY PFPN(t_{final}) AND AVERAGE RATE DENOTED BY Δt.

Test case	PFPN(t_{final})	Δt (min)
Individual power system	0.47	7.25
Coupled system	1	0.37

previous study [35], which models the combating virus spread in wireless sensor networks.

Figs. 5 (a) and (b) show the dynamical profiles of cascading failures in the cyber network (a computer malware infected B_1 at $t = 0$) and the uncoupled power system (node A_1 removed at $t = 0$), respectively. From Fig. 5(b), we see that the failure propagates very slowly in the uncoupled power network before $t = 330$ min and that an abrupt increase of PFPN(t) occurs around $t = 330$ min, indicating that numerous power nodes failed in a short time during the failure cascading process. Compared with the historical data recorded in the 2003 power blackout in the United States and Canada [34] and two blackouts in July and August 1996 of Western North America [33], the results in Fig. 5(b) show similar typical profiles of cascading failures. According to equation (19), the growth rate of PFPN(t) is related to the sum of the tripping rates, i.e., $r^* = \sum \lambda_i$ in this case. This abrupt change around $t = 330$ min is caused by the failure of some critical element in the power system leading to drastic power flow changes. We view the process where one element's state change causes redistribution of the overall power flows in the whole network as a *global* process, and this *global* process can cause a drastic increase of failure propagation rate in the system. Fig. 5(a) shows that PFCN(t) grows smoothly. According to equation (19), the growth rate of PFCN(t) is related to the sum of the infection rates, i.e., $r^* = \sum \mu_i$ in this case. We view the process where the infected node only influences its neighbouring nodes as a *local* process, which cannot cause any drastic change in r^*. Thus, PFCN(t) rises gradually. Clearly, the failure propagation patterns for the power network and the cyber network are dependent on the spreading mechanisms.

Fig. 5(c) shows the failure propagation in the coupled system initiated by a computer malware injected at cyber node B_1 at $t = 0$. The failure propagation in the coupled system is the combined effect of the above two mechanisms as well as the interactions between these two different networks. The propagation profile displays another interesting feature: PFPN(t) has a multiple-step staircase like growing pattern, clearly showing the typical step propagation pattern of cascading failures in the power network being repeatedly triggered by cyber attacks. Table II lists the averaged results of 100 repeated simulations of cascading failures in the individual power system and the coupled system, respectively. Here, PFPN(t_{final}) refers to the percentage of failed power nodes in the final state, and Δt is the average time interval when PFPN(t) is increased by one per cent. It can be seen that the coupled system can have a larger area of blackouts as well as a much faster failure spreading rate than the standalone power network.

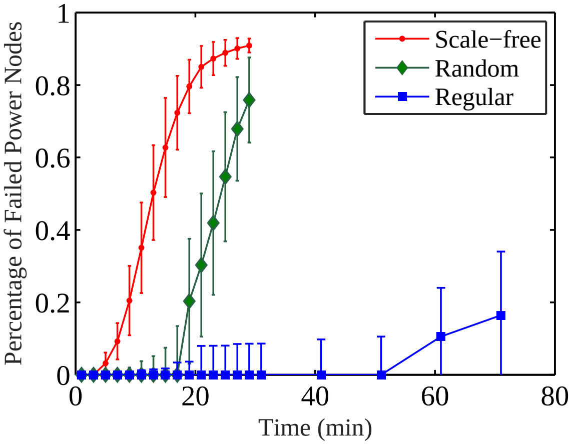


Fig. 7. Comparison of the extents of cascading failures in power grid coupled with cyber network of different topological structures.

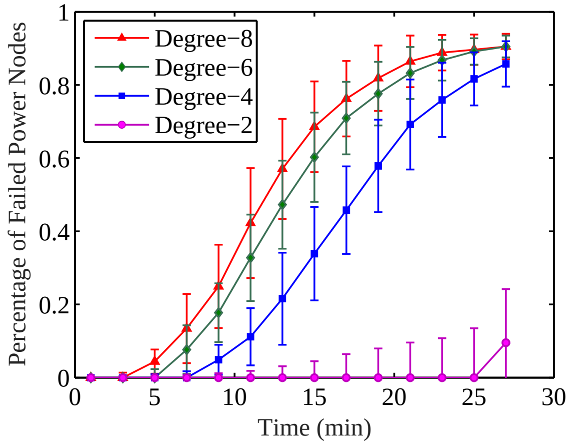
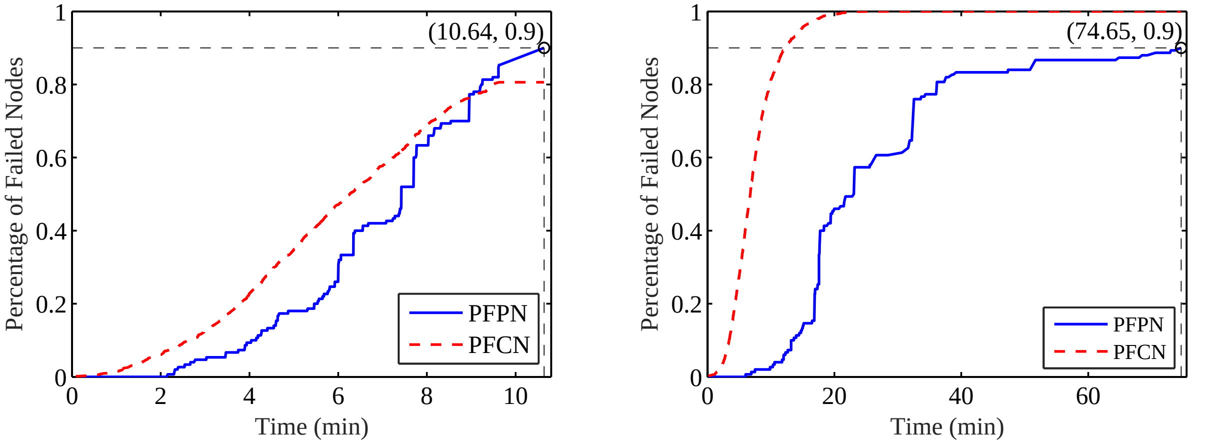


Fig. 8. Comparison of the extents of cascading failures in power grid coupled with cyber network of different average node degrees.

B. Effects of Cyber Network Structures

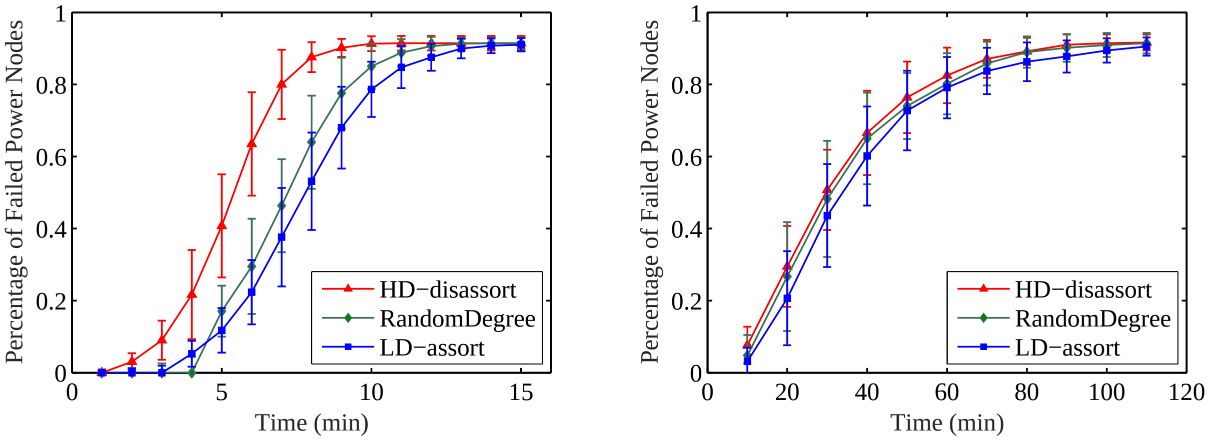
In this section, we investigate the influence of cyber network structure on the cascading failure propagation in the coupled system. We generate cyber networks of three classic typologies: *scale-free* (SF) network [36], *random* network [37] and *regular* network. The average node degree of all these cyber networks are fixed at 6. The size of the network is 1500. We use a random coupling pattern between the cyber network and the power grid in this section, i.e., 150 cyber nodes are chosen randomly from the cyber network to connect the power nodes. The infection rate β_{ij} is set as 0.1 min^{-1}.

Fig. 6 shows the propagation profiles of cascading failures for three different cyber network structures, organized in three sets of charts, namely Figs. 6(a), (b), (c); Figs. 6(d), (e), (f); and Figs. 6(g), (h), (i). Specifically, Figs. 6(a), (d) and (g) show the malware spreading in the different types of cyber networks. We see that the regular cyber network has the slowest spreading rate with an almost linear growth profile. In terms of the spreading rate, the scalefree network is the fastest



(a) (b)

Fig. 9. Spreading patterns in the coupled system under (a) strong attack with $c(t) = 0.3$ min^{-1}; and (b) weak attack with $c(t) = 0.01$ min^{-1}.



(a) (b)

Fig. 10. Extents of cascading failure in the coupled system under (a) strong attack with $c(t) = 0.3$ min^{-1}; and (b) weak attack with $c(t) = 0.01$ min^{-1}.

and the regular network is the slowest. Figs. 6(b), (e) and (f) show the growing profiles of PFPN(t) in the uncoupled power system, which are similar to the typical profile shown earlier in Section IV-A. Figs. 6(c), (f) and (i) show the multiple-step staircase pattern in the failure propagation profile of the power network coupled with the cyber network. This again clearly shows the typical step propagation pattern of cascading failures in the power network being repeatedly triggered by cyber attacks.

Table III shows the averaged PFPN(t_{final}) and $\triangle t$ of 100 repeated simulations in the above three different coupled systems, respectively. Furthermore, Fig. 7 shows the averaged PFPN(t) and the deviations of a number of repeated simulations in the three coupled systems: UIUC-150 Bus System coupled with cyber network of different topological structures. Results show that when attacked by cyber malwares, the power system coupled with scale-free cyber network displays the most severe cascading failure.

TABLE III
COMPARISON ON SEVERITY OF CASCADING FAILURES BETWEEN THE ISOLATED POWER GRID AND THE COUPLED SYSTEM IN TERMS OF CASCADING FAILURE EXTENT DENOTED BY PFPN(t_{final}) AND AVERAGE RATE DENOTED BY $\triangle t$.

Topology of synthesized cyber network	PFPN(t_{final})	$\triangle t$ (min)
Scale-free	1	0.32
Random	1	0.44
Regular	1	6.76

It has been shown that most of the cyber networks in the real world have a scale-free structure. We evaluate the effect of the average node degree of the scale-free cyber network on the vulnerability of the power system coupled with it. We generate four scale-free networks of average node degree 2, 4, 6, and 8. Fig. 8 reveals that if the average node degree of a scale-free cyber network is higher, the system is more vulnerable to attack with more failure transitions.

C. Effects of Coupling Patterns

Finally, we analyze how the coupling patterns between the two interdependent networks influence the dynamic propagation of cascading failures in power networks. Since the cyber network is normally much larger than the power network in terms of the number of nodes ($q \gg p$), we consider the coupling of all power nodes with 10% of cyber nodes in a one-to-one fashion. Three different coupling patterns are considered:

1) *High-degree cyber coupling:* Nodes in the cyber network are sorted in descending order of node degree, and the power nodes are sorted in ascending order (which is immaterial as all power nodes are coupled), namely, $\deg(A_1) \leq \deg(A_2) \leq \cdots \leq \deg(A_p)$ and $\deg(B_1) \geq \deg(B_2) \geq \cdots \geq \deg(B_q)$, where deg(.) denotes degree of the node. Then, coupling is established by connecting A_i and B_i $(i = 1, 2, \cdots p)$.
2) *Random-degree-node coupling:* Randomly choose p nodes out of the q cyber nodes to connect the power nodes.
3) *Low-degree cyber coupling:* Similar to the first case, but with nodes in the cyber network sorted in ascending order of node degree such that the power nodes are coupled with low-degree cyber nodes.

Furthermore, in order to analyze how the coupling strength $c_i(t)$ influences the cascading failures, we study two cases: (1) strong attack with $c_i(t)$ set as 0.3 min^{-1}; (2) weak attack with $c_i(t)$ set as 0.01 min^{-1}.

Figs. 9(a) and (b) show the failure propagation patterns under strong and weak attacks, respectively, for random-degree-node coupling. Under the strong attack condition, PFCN(t) is close to PFPN(t), meaning that an infected cyber node can lead to breakdown of power nodes very quickly (Fig. 9(a)). However, under weak attack condition, as shown in Fig. 9(b), PFCN(t) and PFPN(t) are farther apart. In terms of failure spreading rates, we see that applying strong attack, the cascading failure incurs more severe damage and occurs more rapidly.

Fig. 10 shows the averaged PFPN(t) profiles and their deviations of a number of repeated simulation runs at several specific time points for the three coupling patterns. From Fig. 10(a), under a strong attack condition (high coupling strength), high-degree dis-assortative coupling leads to a more vulnerable coupled system, while low-degree assortative coupling gives a more robust coupled system. However, under a weak attack condition, as shown in Fig. 10(b), the effect of coupling patterns is less significant.

V. Conclusions

The development of future smart grids is inevitably involving more computer control and communication technologies. The coupling of power networks with other networks of computers and even future IoT (Internet of Things) will have a significant impact on the safe and reliable operation of this important infrastructure. This paper presents a novel stochastic model to investigate the characteristics of cascading failures in smart grids triggered by cyber malware attacks. Our study shows that cyber attacks could incur much more severe damages to power networks and power blackouts could occur much more rapidly when power networks are coupled with cyber networks. Our findings also demonstrate the importance of understanding how coupling weakens robustness and the various factors that affect the extent and rapidity of cascading failure propagation in coupled power networks.

Appendix: Transition Process

We consider network state transitions in an infinitesimal time interval dt. Suppose $S(t) = N_S$. Thus, $S(t + dt)$ is the network state after a duration of dt.

(i) Omitting the higher order (with order 2 and higher) items of dt, the probability that no element undergoes a state transition after dt can be written as

$$P[S(t+dt) = N_S \,|S(t) = N_S\,] = \prod_{i=1}^{n} (1 - r_i(t)dt)$$

$$\approx 1 - \sum_{i=1}^{n} r_i(t)dt$$

(ii) The probability that only one state transition channel (channel k) exists in the state transition list after dt, i.e., only element k can transit, can be written as

$$P[S(t+dt) = M_S \,|S(t) = N_S\,] = \prod_{i=k} r_i(t)dt \prod_{i\neq k} (1 - r_i(t)dt)$$

$$\approx r_k(t)dt$$

where M_S denotes the network state that N_S transits to through one channel.

(iii) The probability that two or more state transition channels occur after dt is given by

$$P[S(t+dt) = R_S \,|S(t) = N_S\,] \approx 0$$

where R_S denotes the network state that N_S transits to through two or more channels in the state transition list. Thus, there is at most one element state transition at a time.

References

[1] X. Yu and Y. Xue, “Smart grids: A cyber–physical systems perspective,” *Proc. of IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016.

[2] R. Baheti and H. Gill, “Cyber-physical systems,” *Impact of Control Tech.*, vol. 12, pp. 161–166, Mar. 2011.

[3] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid,” *Proc. of IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[4] C. Lu, R. Rajkumar, and E. Tovar, “Guest editorial special section on cyber-physical systems and cooperating objects,” *IEEE Trans. Ind. Inform.*, vol. 8, no. 2, pp. 378–378, May 2012.

[5] H. Gharavi, H.-H. R. Chen, and C. Wietfeld, “Guest editorial special section on cyber-physical systems and security for smart grid,” *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2405–2408, Sept. 2015.

[6] D. M. Nicol, “Hacking the lights out,” *Scientific Amer.*, vol. 305, no. 1, pp. 70–75, 2011.

[7] M. Zeller, “Myth or realitydoes the aurora vulnerability pose a risk to my generator?” in *Proc. Ann. Conf. Protect. Relay Eng.*, 2011, pp. 130–136.

[8] R. M. Lee, M. J. Assante, and T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. SANS ICS and Electricity Information Sharing and Analysis Center, 2016.

[9] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information,” *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

[10] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava, “Analyzing the cyber-physical impact of cyber events on the power grid,” *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2444–2453, Sept. 2015.

[11] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, “Protecting smart grid automation systems against cyberattacks,” *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 782–795, Dec. 2011.

[12] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. Garcia, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sept. 2015.

[13] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Trans. Power Syst.*, vol. 27, no. 2, p. 631, May 2012.

[14] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability analysis," *Reliab. Eng. Syst. Safety*, vol. 95, no. 12, pp. 1335–1344, 2010.

[15] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *Int. J. Crit. Infrastruct.*, vol. 4, no. 1-2, pp. 63–79, 2008.

[16] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, 2010.

[17] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016.

[18] M. Rahnamay-Naeini and M. Hayat, "Cascading failures in interdependent infrastructures: An interdependent markov-chain approach," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 1997–2006, Mar. 2016.

[19] X. Zhang and C. K. Tse, "Assessment of robustness of power systems from a network perspective," *IEEE J. Emerg. Sel. Top. Circ. Syst.*, vol. 5, no. 3, pp. 456–464, Sept. 2015.

[20] V. Karyotis and M. Khouzani, *Malware Diffusion Models for Modern Complex Networks: Theory and Applications*. Morgan Kaufmann, 2016.

[21] I. Dobson, "Estimating the propagation and extent of cascading line outages from utility data with a branching process," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 2146–2155, Nov. 2012.

[22] Q. Chen, C. Jiang, W. Qiu, and J. D. McCalley, "Probability models for estimating the probabilities of cascading outages in high-voltage transmission network," *IEEE Trans. Power Syst.*, vol. 21, no. 3, pp. 1423–1431, Mar. 2006.

[23] S. Pahwa, C. Scoglio, and A. Scala, "Abruptness of cascade failures in power grids," *Sci. Rep.*, vol. 4, 2014.

[24] M. J. Eppstein and P. D. Hines, "A random chemistry algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

[25] M. Anghel, K. A. Werley, and A. E. Motter, "Stochastic model for power grid dynamics," in *Proc. Hawaii Int. Conf. Syst. Sci.*, 2007, pp. 113–113.

[26] Z. Wang, A. Scaglione, and R. J. Thomas, "A markov-transition model for cascading failures in power grids," in *Proc. Hawaii Int. Conf. Syst. Sci.*, 2012, pp. 2115–2124.

[27] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, "Stochastic analysis of cascading-failure dynamics in power grids," *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1767–1779, Jul. 2014.

[28] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, S. Mei, W. Wei, and L. Ding, "Risk assessment of multi-timescale cascading outages based on markovian tree search," *arXiv preprint arXiv:1603.03935*, 2016.

[29] Y. Sun, P. Wang, L. Cheng, and H. Liu, "Operational reliability assessment of power systems considering condition-dependent failure rate," *IET Gen. Trans. Dist.*, vol. 4, no. 1, pp. 60–72, 2010.

[30] Y. Li, Y. Zhou, F. Liu, Y. Cao, and C. Rehtanz, "Design and implementation of delay-dependent wide area damping control for stability enhancement of power systems," *IEEE Trans. Smart Grid*, In Press, DOI:10.1109/TSG.2015.2508923.

[31] Y. Li, F. Liu, and Y. Cao, "Delay-dependent wide-area damping control for stability enhancement of hvdc/ac interconnected power systems," *Control Engineering Practice*, vol. 37, pp. 43–54, 2015.

[32] *UIUC 150-Bus System*, accessed on Jul. 2016. [Online]. Available: http://icseg.iti.illinois.edu/synthetic-power-cases/uiuc-150-bus-system/.

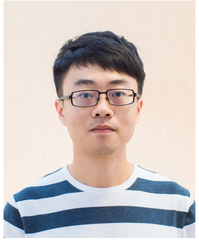
[33] E. C. Eakeley *et al.*,"1996 system disturbances," North Amer. Elect. Rel. Council, Disturb. Anal. Working Group, Atlanta, GA, USA, Tech. Rep., 2002. [Online]. Available: http://www.nerc.com/pa/rrm/ea/System%20Disturbance%20Reports%20DL/1996SystemDisturbance.pdf

[34] U.S.-Canada System Outage Task Force, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," U.S. Dept. of Energy and Nat. Res. Canada, Tech. Rep., 2004. [Online], Available: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf.

[35] S. Tang, "A modified SI epidemic model for combating virus spread in wireless sensor networks," *Int. J. of Wireless Information Networks*, vol. 18, no. 4, pp. 319–326, 2011.

[36] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[37] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publ. Math. Inst. Hungar. Acad. Sci*, vol. 5, pp. 17–61, 1960.



Xi Zhang received the BEng degree in electrical engineering from Beijing Jiaotong University, Beijing, China, in 2013. He is currently pursuing the PhD degree in the Department of Electronic and Information Engineering, Hong Kong Polytechnic University, Hong Kong.

His research interests include nonlinear analysis of power systems, modelling of electrical networks, and applications of complex networks in the assessment of robustness of power systems.

Dong Liu received the B. Eng (Hons) in Electronic Engineering with first class from The Hong Kong Polytechnic University, Hong Kong, in 2014 and B. Eng in Microelectronics from Sun Yat-sen University, Guangzhou, China, in 2014. He is currently pursuing the Ph.D. degree with the Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong.

His research interests include applications of complex networks in the assessment of robustness of power systems and cyber physical systems.

Choujun Zhan received the BS degree in automatic control engineering from Sun Yat-Sen University, Guangzhou, China, in 2007 and the PhD degree in electronic engineering from City University of Hong Kong in 2012. After graduation, he worked as a postdoctoral fellow at the Hong Kong Polytechnic University. Since fall 2016, he has been Associate Professor with the Department of Electronic Communication and Software Engineering, Nanfang College of Sun Yat-Sen University, Guangzhou, China. His research interests include complex networks, collective human behavior and systems biology.

Chi K. Tse (M'90–SM'97–F'06) received the BEng (Hons) degree in electrical engineering and the PhD degree from the University of Melbourne, Australia, in 1987 and 1991, respectively. He is presently Chair Professor at the Hong Kong Polytechnic University, Hong Kong, with which he was Head of the Department of Electronic and Information Engineering from 2005 to 2012.

He is author/co-author of 10 books, 20 book chapters and over 500 papers in research journals and conference proceedings, and holds 5 US patents. He has served and serves as the Editor-in-Chief of the IEEE Transactions on Circuits and Systems II (2016-2017), the *IEEE Circuits and Systems Magazine* (2012-2015), the Editor-in-Chief of the *IEEE Circuits and Systems Society Newsletter* (since 2007), an Associate Editor of three IEEE Journal/Transactions, and the Editor of the *International Journal of Circuit Theory and Applications*. His research interests include power electronics, nonlinear circuits, and complex network applications.