Cascading failure dynamic of cyber-physical power system considering malware attacks

Meie Shen\textsuperscript{1}, Xingle Gao\textsuperscript{2,3} and Minfang Peng\textsuperscript{2}

\textsuperscript{1}Beijing Information Science and Technology University, Beijing, China
\textsuperscript{2}Hunan University, Changsha, China
\textsuperscript{3}Email: xingle_gao@163.com

Abstract. With the development of cyber-physical power system, cyber security has a serious impact on the operation of power system. In this paper, a stochastic cascading failure model considering the structural and dynamical characteristics of cyber-physical power system is proposed. The model takes into account the community structure of networks, the heterogeneity of network nodes and the complex interdependence of coupling networks. Moreover, the malware spreading in the cyber network and the power flow redistribution in the power grid are considered to describe the dynamic physical processes of the system, and a stochastic method is adopted to describe the operating state transition of network components. Simulation results indicate that the cascading failure of coupled system is the result of malware attacks repeatedly triggering the power grid, and cyber coupling will aggravate the severity of grid failure propagation.

1. Introduction

Smart grid is a typical cyber-physical system (CPS) [1], which is supported by advanced cyber networks and delivers power to final users. The introduction of information and communication technology (ICT) improves the operating efficiency of the power system, but also brings potential negative impact on the safety of the power grid. Cyber security has become a key challenge for power system due to the fact that the interaction of communication system makes smart grid vulnerable to cyber attacks. For example, in December 2015, a serious blackout occurred in Ukraine due to the computer malware attack from the cyber network, which indicated that the cyber attack on the cyber-physical power system (CPPS) was no longer a fictional event.

As one of the most complex artificial networks in the world, using the complex network theory to analyze the topological and dynamical characteristics of power system has become a research hotspot. At present, a large number of studies have been conducted on the cascading failure analysis of power grid and cyber network [2]-[3], but the relevant research mainly focuses on the cascading failure of single networks. However, the future smart grid will largely depend on the secure and efficient operation of the interdependent power equipment and cyber network, so researchers gradually turn their attention to the cascading failure analysis of interdependent networks. Buldyrev et al. [4] proposed the concept of interdependent network and modeled the cascading failure mechanism of interdependent network based on the percolation theory. Chen et al. [5] took into account the operational settings of networks and developed a failure model to investigate the cascading failures in the interdependent network. Although the above studies focused on the coupled system composed of power grid and cyber network, the impacts of malware attacks on the operation of power system was not considered. Due to the coupling of
the power grid and the cyber network, the failure propagation of smart grid will be inevitably affected by malware attacks. Therefore, it is becoming more and more crucial to study the impacts of malware attacks on the dynamics of coupled system. Zhang and Liu et al. [6] considered the impacts of power overloading and cyber attack on the failure propagation and investigate the cascading failure of coupled systems. However, the model in their work ignores the community structure of the interdependent networks and does not take into account the effects of anti-malware actions.

In this paper, we take into account the structural and dynamical characteristics of CPPS, and investigate the impact of malware attacks on the failure propagation of coupled system. First, considering the community structure of the networks and the functional characteristics of the components in the coupled system, we establish a heterogeneous interdependent modular network. Then, we analyze the failure mechanism of heterogeneous nodes in terms of topology. Moreover, we analyze the malware spreading in the cyber network, and calculate the power flow distribution of the power grid. Considering the randomness of the failure propagation in CPPS, a stochastic method is adopted to describe the operating state transition of the components in the coupled system. This paper provides a basis for investigating the impact of cyber attacks on the CPPS.

![Figure 1. Interdependent modular network model of CPPS.](image)

2. Network model
Power grid generally meets the requirements of partition running and regional control. Therefore, the power grid has typical community structure characteristics. Specifically, the maximum modularity [7] of the network is usually used to characterize the strength of the community structure, and the closer the maximum modularity is to 1, the stronger the community structure of the network is. Generally, when the maximum modularity of a network is greater than 0.3, it can be considered that the network has obvious community structure. In this paper, we use the GN algorithm [8] to analyze the community structure of power grid. Using GN algorithm, we find that the maximum modularity of the IEEE 118 bus system can reach 0.7195. Therefore, it can be considered that IEEE 118 bus system has obvious community structure. In addition, power grids in different partitions are generally controlled by local communication systems. Therefore, the CPPS network model can be expressed as a modular interdependent network, as shown in Figure 1, which contains two coupled community networks. The cyber network in the coupled system is mainly responsible for monitoring the power grid. The control centers and communication stations in the cyber network can be abstracted as control nodes and relay nodes respectively according to their functions. We assume that each modular interdependent network contains a regional control center. Similarly, the power grid is responsible for power supply. The physical equipment in the power grid, such as power plants, substations and convergence buses can be abstracted as generation nodes, transmission nodes and consumer nodes respectively. The interdependence between the two networks is depicted by the vertical black dashed lines shown in Figure 1. Note that the control nodes in the cyber network are usually equipped with sufficient standby power, which can be regarded as autonomous nodes decoupling from power grid.
3. Cascading failure mechanism

3.1. Topological failure
Considering the heterogeneity of network nodes, the cyber nodes in each subnetwork should meet the logical connectivity of communication components, that is, each subnetwork in the cyber network should contain at least one control node and one relay node, otherwise the nodes in the subnetwork will be regarded as failure. Similarly, each subnetwork in the power grid should contain at least one generation node and one consumer node, otherwise the subnetwork will be considered as failure. In addition, referring to the interaction mechanism between cyber network and power grid proposed in [4] and [5], when the corresponding coupling power node of a cyber node fails, the cyber node will lose power supply and fail, and when the cyber node of a power node fails, the power node will fail to receive the monitoring of control center and thus fail.

3.2. Malware spreading in cyber network
In the cyber network, a normal cyber node can be infected by malware through its infected neighbor nodes, and the infection rate is related to the number of infected neighbor nodes. The infection rate of cyber node $i$ can be described as follows:

$$\delta_i(t) = \sum_{j \in \Omega} \beta_{ij}$$

(1)

where $\Omega$ represents the set of all infected nodes connected with cyber node $i$, $\beta_{ij}$ represents the infection rate of infected node $j$ infecting its neighbor node $i$. In this paper, we consider the repair of the infected cyber nodes due to the large use of antivirus software. Here, we assume that the recovery rate of the infected node $i$ is $r_i$. Note that the repaired cyber node may be re-infected by other infected nodes.

In addition, due to the interaction between the power grid and the cyber network, when the corresponding coupling power node of a cyber node fails, the cyber node will be completely removed from the network, so the node will not be infected by malware or infect other cyber nodes. Considering the key role of the control center, we assume that the control nodes are immune nodes that can be immune to malware. Moreover, when the corresponding coupling cyber node of a power node is infected by malware, the infected cyber node can take malicious actions on the coupling power node. The probability that a power node is attacked by the infected cyber node is $c_i$.

3.3. Overload failure in power network
In the cascading process, it is difficult to obtain power flow information by repeatedly solving full nonlinear equations. Therefore, we ignore the non-linear characteristics of electrical components and adopt the DC power flow model to calculate the flow dispatch of power grid. In this paper, we consider the overload failures of power lines as they are one of the most observable signs of cascading failures. Note that in the process of power flow calculation, if the island’s power is unbalanced, it is necessary to balance the power before determining the effectiveness of power lines. In this paper, we use the power balance algorithm proposed in [9]. The failure rate of the lines is not constant, but related to their load state. Specifically, if line $i$ is heavily overloaded, it will be tripped more rapidly than those with lighter overloading. The failure rate of power line $i$ can be described as:

$$\lambda_i(t) = \begin{cases} a_i \left( \frac{L_i(t)}{C_i} - 1 \right), & L_i(t) > C_i \\ 0, & L_i(t) < C_i \end{cases}$$

(2)

where $a_i$ is the basic tripping rate, $L_i(t)$ is the power loading of line $i$, $C_i$ is the load capacity of line $i$.

3.4. Stochastic operating state transition
In this section, we analyze the operating state transition of network components. The topological failure is caused by the fact that the network nodes fail to meet the logical connectivity of network nodes.
Therefore, topological failure can be regarded as deterministic state transition that does not consume time. In addition, there are four probabilistic state transition events during the operation of system, namely, the infection of cyber node, the overload failure of power line, the failure of power node caused by coupling infected cyber node, and the repair of infected cyber node. The infection rate of a cyber node is related to the number of infected neighbor nodes. The overload failure rate of a power line is closely related to the overload extent of that line. Moreover, the failure of power node caused by coupling infected cyber node and the repair of the infected cyber node are also probabilistic events. We use a stochastic method to describe the probabilistic state transition events, and the time intervals between state transition and the sequence of state transition are stochastic. We assume that there is only one stochastic state transition at a time.

Let $\Omega_0$ be the set of all components that may change their operating state. The probability that no component changes its operating state in time interval $(t, t + \tau)$ is given by

$$S(\tau) = 1 - \sum_{i \in \Omega_0} u_i(t) \tau$$

where $u_i(t)$ is the transition rate of component $i$ at time $t$ [2].

Similarly, the probability that no component change their operating state in time interval $(t, t + \tau + \Delta t)$ is

$$S(\tau + \Delta t) = S(\tau)(1 - \sum_{i \in \Omega_0} u_i(t)\Delta t)$$

Taking the infinitesimal $\Delta t$ to 0, we get

$$\frac{dS(\tau)}{d\tau} = \lim_{\Delta \rightarrow 0} \frac{S(\tau + \Delta t) - S(\tau)}{\Delta t} = - \sum_{i \in \Omega_0} u_i(t)S(\tau)$$

Solving the above differential equation, we get

$$S(\tau) = e^{-\sum_{i \in \Omega_0} u_i(t)\tau}$$

Thus, the probability of state transition occurring in $(t, t + \tau)$, denoted by $F(\tau)$, is given by

$$F(\tau) = 1 - S(\tau) = 1 - e^{-\sum_{i \in \Omega_0} u_i(t)\tau}$$

Suppose the next state transition occurs at time $\tau$. We generate a random number $z_1$ uniformly in $(0, 1)$, and the failure time $\tau$ is given as

$$\tau = F^{-1}(z_1) = \frac{\ln(1 - z_1)}{-\sum_{i \in \Omega_0} u_i(t)}$$

where $z_1 = F(\tau)$. Suppose there are $n$ components that may change their operating state, then the component $k$ will be selected when it fits the equation:

$$\frac{\sum_{j=0}^{k-1} u_j(t)}{\sum_{i \in \Omega_0} u_i(t)} \leq z_2 \leq \frac{\sum_{j=0}^{k-1} u_j(t)}{\sum_{i \in \Omega_0} u_i(t)}$$

where $z_2$ is a random number generated uniformly in interval $(0, 1)$. Note that the value of $u_i$ can be $\delta_i$, $r_i$, $c_i$ and $\lambda_i$ in this study, and $\sum u_i(t)$ represents the sum of transition rate of all operating components.

3.5. Simulation algorithm

Therefore, the cascading failure process of CPPS can be described as follows:
1) Initialization: First, the network structure and coupling information of coupled system, as well as physical and operational parameter of the cyber network and the power network are set up.

2) Malware Injection: We assume that the cascading failures of coupled system are caused by malware attacks. Thus, the initial network failure is to inject malware into the cyber network.

3) Malware Diffusion: In order to get enough cyber nodes infected, we assume that malware will spread in the cyber network for a period of time before attacking the power grid. Here, $t_d$ is set as the infection stage before attacking the power grid, during which only cyber node infection occurs.

4) Cyber Attack: After $t_d$, malware will launch attack to the power grid, and all failure modes or state transition events may occur in the process. The iterative process is as follows:

(a) Topological failure detection. Identify the connectivity of power nodes, and remove the nodes that do not meet the connectivity conditions and their coupling cyber nodes. Then, identify the connectivity of cyber nodes, and remove the nodes that do not meet the connectivity conditions and their coupling power nodes. Repeat these two processes until all nodes satisfy connectivity conditions.

(b) Stochastic state transition detection. First, detect the power balance of each island in the remaining power grid and calculate the actual loads of power lines. Second, detect the malware contagion of each subnetwork in the remaining cyber network and calculate the infection rate of cyber nodes. Third, detect the infected cyber nodes in the remaining cyber network to determine the cyber nodes that may be repaired and the power nodes that may be attacked. Then, the ratio of all operating state transition in the coupled system is obtained.

(c) If there is a state transition event, select the transition time and transition component using equations (8) and (9), and return to step (a); otherwise, output the final network.

4. Case study

4.1. Settings
In this section, we use the proposed model to study the cascading failure mechanism of coupled system and further investigate the influence of malware attacks on the cascading failure of CPPS. According to the above analysis, we can find that IEEE 118 bus system can be divided into 9 community partitions. Previous studies have shown that many real-world cyber networks show scale-free properties. Based on the grid partition result, we use the extended network model proposed in [10] to build a modular scale-free cyber network. The relay nodes of each community in the cyber network are randomly coupled with the power nodes in the grid partition. The capacity of each line in the power network is set as 1.2 times its respective initial load, and the basic tripping rate $a_i$ is set as $0.21 \text{ min}^{-1}$ for the power grid. The malware infection rate $\beta_{ij}$ is set as $0.5 \text{ min}^{-1}$, the recovery rate $r_i$ of the infected cyber node is set as $0.1 \text{ min}^{-1}$, the probability $c_i$ of the infected cyber node attacking the power node is set as $0.05 \text{ min}^{-1}$, and the malware diffusion time $t_d$ is set as 2 min.

4.2. Failure propagation in the coupled system
First, we compare the cascading failure propagation in the power grid, cyber network and interdependent network. In order to illustrate the universality of the results, we choose different recovery rates of cyber nodes for analysis. Figure 2 shows the failure propagation profiles of different networks. Figure 2 (a), (d) and (g) show the failure propagation profiles of the uncoupled IEEE 118 bus system. It can be found that the failure profiles show the same cascading pattern as the results recorded in [11], that is, the initial phase of failure propagation is relatively slow, and then followed by a sharp escalation of cascading failure. The reason is that the failure of one component can lead to the redistribution of power flow in the whole power grid, and the failure of some critical components may lead to the drastic change of the power flows, which may lead to the drastic increase of failure propagation. Figure 2 (b), (e) and (h) show the malware spreading in the cyber network at different recovery rates. We can find that due to the dynamic process of malware infection and node repair, the failure profiles in the cyber network show a downward trend of fluctuation, and finally reach a stable state. In addition, the failure propagation profile of the cyber network changes smoothly, and there is no
sharp escalation like that in the power network. The reason is that the infected nodes in the cyber network only affect their neighbor cyber nodes, which is a local dynamic process and will not cause the drastic change of infection rate. We also find that with the increase of recovery rate, the spreading speed of malware and the failure severity of cyber network are all decreased.

Figure 2 (c), (f) and (i) show the failure propagation profiles in the interdependent network at different recovery rates. We can find that the results share the same characteristic profile, where the growing rate of failure scale is not uniform and the operating nodes present a step-down staircase pattern. The failure of the power grid in the coupled system is not only related to the flow overloading of the power lines, but also related to the malware attacks from the cyber network. The failure profiles clearly show the failure propagation pattern that the power grid is repeatedly triggered by the cyber attacks. In addition, by comparing Figure 2 (a), (d), (g) with Figure 2 (c), (f), (i), we can find that the coupled system has a larger failure proportion and a faster failure propagation rate than the single power grid, that is, cyber coupling aggravate the severity of cascading failure in the power grid. Table 1 shows the average results of 100 repeated simulations of cascading failures in the interdependent network at different recovery rates. Here, $\Delta t$ is the average time interval when the failure proportion of power nodes in the interdependent network is increased by 1%. We can find that with the increase of the recovery rate of cyber nodes, the failure propagation rate of the coupled system is decreased.

![Figure 2. Failure propagation patterns. (a), (d), (g): failure propagation in (uncoupled) power grid; (b), (e), (h): malware spreading in cyber network, with $r_i = 0.1$, $r_i = 0.2$, $r_i = 0.3$, respectively; (c), (f), (i): failure cascading in the interdependent network, with $r_i = 0.1$, $r_i = 0.2$, $r_i = 0.3$, respectively.](image-url)
Table 1. The average failure rates of interdependent networks under different recovery rates of cyber nodes.

| Recover rate (min⁻¹) | Δt (min) |
|----------------------|----------|
| r_i = 0.1            | 0.982    |
| r_i = 0.2            | 1.127    |
| r_i = 0.3            | 1.298    |

5. Conclusions
With the rapid development of smart grid, the power grid is more and more dependent on the communication system. Cyber security has become a major challenge for the safe and reliable operation of the power system. Taking into account the topological structure of coupled system, the malware attacks of cyber network, and the flow overloading of power grid, we propose a stochastic cascading failure model reflecting the space-time features of the failure components to describe the failure process of CPPS. The results show that the cascading failure of the coupled system presents a "staircase" failure pattern in which the malware attacks repeatedly trigger the power grid, and cyber coupling will aggravate the severity of cascading failure in the power grid. This study provides an idea for the dynamic analysis of cascading failure in the coupled system.

Acknowledgments
This work was supported by the NSFC (No.61973107 and No.61472128).

References
[1] Qu C, Chen W, Song J B and Li H 2015 Distributed data traffic scheduling with awareness of dynamics state in cyber physical systems with application in smart grid IEEE Trans. Smart Grid vol. 6 no. 6 pp. 2895-2905
[2] Zhang X, Zhan C and Tse C K 2017 Modeling the dynamics of cascading failures in power Systems IEEE J. Emerg. Sel. Topics in Circ. Syst. vol. 7 no. 2 pp. 192-204
[3] Ren W, Wu J, Zhang X, Lai R and Chen L 2018 A Stochastic Model of Cascading Failure Dynamics in Communication Networks IEEE Trans. Circuits Syst. II, Exp. Briefs vol. 65 no. 5 pp. 632-636
[4] Buldyrev S V, Parshani R, Paul G, Stanley H E and Havlin S 2010 Catastrophic cascade of failures in interdependent networks Nature vol. 464 pp. 1025-1028
[5] Chen Z, Wu J, Xia Y and Zhang X 2018 Robustness of interdependent power grids and communication networks: A complex network perspective IEEE Trans. Circuits Syst. II, Exp. Briefs vol. 65 no. 1 pp. 115-119
[6] Zhang X, Liu D, Zhan C and Tse C K 2017 Effects of Cyber Coupling on Cascading Failures in Power Systems IEEE J. Emerg. Sel. Topics in Circ. Syst. vol. 7 no. 2 pp. 228-238
[7] Newman M E J and Girvan M 2004 Finding and evaluating community structure in networks Phys. Rev. E, Stat., Nonlinear. Soft Matter Phys. vol. 69 no. 2 pp. 026113
[8] Girvan M and Newman M E J 2002 Community structure in social and biological networks Proc. Nat. Acad. Sci. U.S.A., vol. 99 no. 12 pp. 7821-7826
[9] Athari M H and Wang Z 2018 Impacts of Wind Power Uncertainty on Grid Vulnerability to Cascading Overload Failures IEEE Trans. Sustain. Energy vol. 9 no. 1 pp. 128-137
[10] Li C and Maini P K 2005 An evolving network model with community structure J. Phys. A: Gen. Phys. vol. 38 no. 45 pp. 9741-9749
[11] Dobson I, Carreras B and Newman D 2005 Branching process models for the exponentially increasing portions of cascading failure blackouts, Proc. Hawaii Int. Conf. Syst. Sci. pp. 1-10