Effects of Malware Attacks on the Cascading Failure of Cyber-physical Power System

Meie Shen¹, Xingle Gao²,* and Minfang Peng²
¹Beijing Information Science and Technology University, Beijing, China
²Hunan University, Changsha, China

*Corresponding author email: xinglegao@hnu.edu.cn

Abstract. In this paper, a stochastic cascading failure model considering the structure and operation of cyber-physical power system is proposed. The model takes into account the community structure and the heterogeneity of networks as well as 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 operational characteristics of the system, and a stochastic method is adopted to describe the operating state transition of network components. In addition, the effects of community structure strength and immunization strategy on the cascading failure of coupled system are studied. The results show that the cascading failure of coupled system is the result of malware attacks repeatedly triggering the power grid. Results also suggest increasing the community structure strength of cyber network helps to suppress the impact of cyber-attacks on the coupled system, and community bridge immunization is the optimal immunization strategy for inhibiting failure propagation in the modular interdependent network.

Keywords: Cascading failure; Cyber-physical system; Interdependent network; Malware.

1. Introduction

The high-speed development of smart grid realizes the deep integration and collaborative work between power grid and communication system, which makes smart grid become a typical cyber-physical system (CPS) [1]. In recent years, the frequent occurrence of cascading failures has seriously affected the normal operation of cyber-physical power system (CPPS), such as the large blackout caused by the failure of cyber network and control system in North America in August 2003. Cyber security has become a key challenge for power system due to the fact that the interaction of cyber network makes smart grid vulnerable to cyber-attacks.

In the past decade, numerous studies have focused on the cascading failure analysis of standalone power grid or cyber network [2]–[4]. However, the physical layer and the cyber layer in the smart grid are highly mutually dependent, so researchers gradually turn their attention to the cascading failure analysis of interdependent networks. Buldyrev et al. [5] proposed the concept of interdependent network and modelled the cascading failure mechanism of interdependent network based on the percolation theory. Chen et al. [6] developed a dynamic model to analyze the cascading failures in the interdependent network. However, the previous work fails to take into consideration the influence of malware attacks on the operation of power system. In fact, the failure propagation of smart grid will be inevitably affected by malware attacks due to the coupling of cyber network.

In this paper, we proposed a stochastic model to investigate the impact of malware attacks on the failure propagation of coupled system. First, we analyze the community structure and the functional characteristics of networks, and establish a network model of CPPS in Section II. Then, considering
the malware spreading in the cyber network and the power flow redistribution in the power grid, we
describe the failure of network components as a state transition process and analyze the failure
mechanism of coupled system in Section III. Finally, the effects of community structure strength and
immunization strategy on the cascading failure of coupled system are studied in Section IV, which
provides a reference for preventing malware attacks.

2. Network Model
In this paper, we introduce the modularity $Q$ to describe the community structure strength of power
grid, and $Q = 0.3$ is usually taken as the lower limit of the obvious community structure. Using GN
algorithm [7], we find that the maximum modularity of the IEEE 118 bus system can reach 0.7195.
Thus, IEEE 118 bus system has a community structure. Power grids in different partitions are
generally controlled by local dispatching systems. Therefore, the CPPS network model can be
expressed as a modular interdependent network. The control centers and communication stations in the
cyber network can be abstracted as control nodes and relay nodes respectively. We assume that each
modular interdependent network contains a control center. Similarly, the power plants, substations and
convergence buses can be abstracted as generation nodes, transmission nodes and consumer nodes
respectively. Note that the control nodes are usually equipped with sufficient standby power, which
can be considered as autonomous nodes.

3. Cascading Failure Mechanism

3.1. State Transitions of Cyber Components
The failure propagation in the interdependent network can be viewed as continuous operating state
transitions of the network components. We assume that a cyber node $C_i$ has three states i.e., state $s_{Ci} \in$
0, 1 and 2. Specifically, $s_{Ci} = 0$ indicates that node $C_i$ operates normally; $s_{Ci} = 1$ means that the node
$C_i$ is infected by a computer malware; $s_{Ci} = 2$ is an invalid state corresponding to the node $C_i$ failing to
meet the logical connectivity of network components. Note that when a node is in state 1, it can infect
its neighbor nodes, while the node in state 2 cannot infect others.

When cyber node $C_i$ is in a normal state, and it has infected neighbor nodes, it can be infected by a
computer malware. Thus, the state transition can be given as

$$T_1 : s_{Ci} = 0 \xrightarrow{\delta} s_{Ci} = 1.$$

where $\delta_i$ denotes the infection rate of cyber node $C_i$ and is defined as

$$\delta_i(t) = \sum_{j \in \Omega} \beta_{ij}. \quad (2)$$

where $\Omega$ represents the set of all infected nodes connected with cyber node $C_i$, $\beta_{ij}$ represents the
infection rate of infected node $j$ infecting its neighbor node $i$.

Each subnetwork in the cyber network should contain both relay node and control node. Considering
the interdependence with power grid, the relay node should connect with a power node. Therefore,
when cyber node $C_i$ is in a normal state, and it fails to satisfies the connectivity conditions of network
components. The state transition can be modelled as:

$$T_2 : s_{Ci} = 0 \xrightarrow{\text{con}} s_{Ci} = 2. \quad (3)$$

where $\text{con}$ denotes that $T_2$ is a deterministic transition. In this case, nodes in the subnetwork change
their states from 0 to 2. Similarly, when $s_{Ci} = 1$, and the cyber node $C_i$ fails to satisfies the logic
connectivity of cyber nodes, there is another state transition,

$$T_3 : s_{Ci} = 1 \xrightarrow{\text{con}} s_{Ci} = 2. \quad (4)$$

In this study, we consider the repair of infected cyber nodes due to the large use of antivirus software.
When cyber node $C_i$ is in an infected state, it can be repaired due to the anti-malware actions, and the
state transition can be described as
where \( r_i \) is the recovery rate of infected cyber node \( C_i \).

### 3.2. State Transitions of Power Components

We assume that a power node \( P_i \) has three states, i.e., state \( s_{Pi} \in 0, 1 \) and 2. Specifically, \( s_{Pi} = 0 \) indicates that node \( P_i \) is in a normal operating state; \( s_{Pi} = 1 \) means that the node \( P_i \) is attacked by the coupling infected cyber node and thus fails; \( s_{Pi} = 2 \) is an invalid state corresponding to the node \( P_i \) failing to meet the logical connectivity of network components.

When power node \( P_i \) is in a normal operating state, and the corresponding coupling cyber node is infected, it may be attacked by the infected cyber node. The state transition can be described as

\[
T_4 : s_{Ci} = 0 \xrightarrow{c_i} s_{Ci} = 1.
\]

where \( c_i \) denotes the attack probability of infected cyber node to the coupling power node.

Each subnetwork in the power grid should contain both generation node and consumer node, and the power node should connect with a cyber node. Therefore, when a normal power node \( P_i \) fails to satisfy the connectivity conditions of network components. The state transition can be modelled as:

\[
T_5 : s_{Pi} = 0 \xrightarrow{\text{con}} s_{Pi} = 1.
\]

Under the condition of \( \text{con} \), nodes in the subnetwork change their states from 0 to 2.

In this study, we consider the overload failures of power lines as they are one of the most observable signs of cascading failures. Let \( s_{Ti} \) denote the possible states of a power line \( T_i \), i.e., \( s_{Ti} \in \{0, 1\} \).

Specifically, \( s_{Ti} = 0 \) represents that line \( T_i \) works normally; \( s_{Ti} = 1 \) means that the line \( T_i \) is tripped by a circuit breaker due to overloading.

When power line \( T_i \) is in a normal state, and the flow through it is overloaded, then it may be tripped by its protective equipment. The state transition process can be given as

\[
T_7 : s_{Ti} = 0 \xrightarrow{\lambda_i} s_{Ti} = 1.
\]

where \( \lambda_i \) denotes the failure rate of power line \( T_i \). In the operation of power system, the failure rate of power lines is not constant, but related to their load state. Therefore, the failure rate of power line \( T_i \) can be described as:

\[
(1 - \left( 1 - \left( 1 - \frac{L_i(t)}{C_i} \right) \right)^{a_i} ) , \quad L_i(t) > C_i \\
0 , \quad L_i(t) < C_i
\]

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 \( T_i \).

### 3.3. Transition Time and Order

From above analysis, we know that \( T_2 \), \( T_3 \) and \( T_6 \) are deterministic state transitions, while \( T_1 \), \( T_4 \), \( T_5 \) and \( T_7 \) are stochastic state transitions. In the cascading process, we first identify deterministic state transitions, and then stochastic state transitions. We use the stochastic model proposed in [2] to describe the stochastic state transition process, and the time for the next transition \( \tau \) is given as

\[
\tau = \frac{\ln(1 - z_i)}{-\sum_{k \in \Omega_0} u_i(t)}
\]

where the random number \( z_i \) is generated uniformly in \((0, 1)\), \( \Omega_0 \) is the set of all components that may change their operating state, \( u_i \) is the state transition rate. Suppose there are \( n \) components that may change their operating state, then the component \( k \) will be selected when it fits the equation:
where the random number $z_2$ is generated uniformly in interval $(0, 1)$.

### 3.4. Simulation Algorithm

The simulation flow chart for cascading failure in CPPS is shown in Figure 1.

![Simulation flow chart of cascading failure in CPPS.](image)

### 4. Case Study

The simulation model used here is Matlab. Using GN algorithm, IEEE 118 bus system can be divided into 9 community partitions. Then, we use the extended network model proposed in [8] 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 power line is set as 1.2 times its respective initial load, and the basic tripping rate $a_i$ is set as 0.21 min$^{-1}$. The malware infection rate $\beta_{ij}$ is set as 0.5 min$^{-1}$, the recovery rate $r_i$ of the infected cyber node is set as 0.1 min$^{-1}$, the probability $c_i$ of the infected cyber node attacking the power node is set as 0.05 min$^{-1}$, and the malware diffusion time $t_d$ is set as 2 min.

![Failure propagation patterns. (a): failure propagation in power grid; (b): malware spreading in cyber network; (c): failure cascading in the interdependent network.](image)

### 4.1. Failure Propagation in the Coupled System

Figure 2 (a) shows the failure propagation curves of the uncoupled IEEE 118 bus system. We can find that the failure propagation is relatively slow before $t = 100$ min, and then a sharp escalation occurs around $t = 100$ min. Figure 2 (b) shows the malware spreading in the cyber network. We can find that due to the dynamic process of malware infection and node repair, the failure curve shows a downward trend of fluctuation, and finally reaches a stable state. Figure 2 (c) shows the failure propagation curve in the interdependent network. We can find that the growth rate of failure scale is not uniform and the
failure process presents a staircase pattern. The failure of the power grid in the coupled system is not only related to the overload of the power lines, but also related to the malware attacks from the cyber network. The failure curve clearly show the failure propagation pattern that the power grid is repeatedly triggered by the cyber-attacks.

4.2. Effect of Community Structure Strength

Figure 3 shows the average failure results of 20 repeated simulation runs at some specific time points for different community structure strengths of cyber networks. We can find that with the increase of connection probability, the severity of cascading failure in the interdependent network increases. The reason is that with the increase of connection probability, the community structure strength of cyber network is weakened, and the connection edges between communities are increased, which increases the diffusion probability of malware among different communities, thus leading to the expansion of attack scale on the power grid and increasing the severity of cascading failure of the coupled system. Therefore, increasing the community structure strength of cyber network can reduce the effects of malware attacks on the coupled system.

![Figure 3](image.jpg)

**Figure 3.** Extents of cascading failure for different community structure strengths in coupled networks.

4.3. Effect of Immunization Strategy

In this study, we define immunization rate $g$ as the ratio of the number of immune relay nodes to the total number of relay nodes in the cyber network. We consider four different immunization strategies and compare them with the non-immune (NI) failure propagation of the coupled system.

1) Random immunization (RI): Randomly select $N_r g$ relay nodes for immunity, where $N_r$ denotes the total number of relay nodes in the cyber network.

2) Acquaintance immunization (AI): Randomly select $N_r g$ relay nodes, and then randomly select a relay node from the neighbor nodes of each selected node for immunity.

3) Target immunization (TI): Calculate the degree centrality of cyber node, and the relay nodes are sorted in descending order, then $N_r g$ nodes are selected according to the ranking order for immunity.

4) Community bridge immunization (CBI): Similarly to case 3, the bridge nodes are sorted in descending order, and then $N_r g$ nodes are selected according to the ranking order for immunity.

Figure 4 shows the average failure results of 20 repeated simulation runs at some specific time points for the four immunization strategies. We can find that compared with RI, AI has a better immune effect, and TI has the best inhibiting effect on the failure propagation in the interdependent networks. Immunizing high-degree nodes will reduce the spreading path of malware, thus decreasing the probability of malware attacking the power grid. However, we need to know the topology information of the whole cyber network before applying TI. From Figure 4, we can find that CBI has similar immune effect compared with TI. The reason is that the malware spreading among communities depends on the bridge nodes between different communities, and the immunity of these nodes can effectively reduce the spread of malware among communities. The application of CBI only needs to know the partial topology of the cyber network.
5. Conclusion
Taking into account the structure of coupled system, the malware attacks of cyber network, and the flow overload of power grid, we propose a stochastic cascading model to describe the failure process of CPPS. The results show that the cascading failure of coupled system presents a "staircase" failure pattern in which the malware attack repeatedly triggers the power grid. Moreover, increasing the community structure strength of cyber network can suppress the spread of malware and reduce the impact of malware attacks on the cascading failure of system. In addition, for modular interdependent networks, community bridge immunization has the best inhibiting effect on the failure propagation in the network. The study provides an idea for the dynamic analysis of cascading failure in the coupled system, and provides a basis for reducing the impact of malware attacks on 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, Distributed data traffic scheduling with awareness of dynamics state in cyber physical systems with application in smart grid, 2015 IEEE Trans. Smart Grid, vol. 6, no. 6, pp. 2895-2905.
[2] Zhang X, Zhan C and Tse C K, Modeling the dynamics of cascading failures in power Systems, 2017 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, A Stochastic Model of Cascading Failure Dynamics in Communication Networks, 2018 IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 65, no. 5, pp. 632-636.
[4] Pahwa S, Scoglio C and Scala A, Abruptness of cascade failures in power grids, 2014 Sci. Rep., vol. 4, pp. 1-9.
[5] Buldyrev S V, Parshani R, Paul G, Stanley H E and Havlin S, Catastrophic cascade of failures in interdependent networks, 2010 Nature, vol. 464, pp. 1025–1028.
[6] Chen Z, Wu J, Xia Y and Zhang X, Robustness of interdependent power grids and communication networks: A complex network perspective, 2018 IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 65, no. 1, pp. 115–119.
[7] Girvan M and Newman M E J, Community structure in social and biological networks, 2002 Proc. Nat. Acad. Sci. U.S.A., vol. 99, no. 12, pp. 7821–7826.
[8] Li C and Maini P K, An evolving network model with community structure, 2005 J. Phys. A: Gen. Phys., vol. 38, no. 45, pp. 9741–9749.