Cascading failures analysis considering extreme virus propagation of cyber-physical systems in smart grids

Hindawi
Complexity
Volume 2019, Article ID 7428458, 15 pages
https://doi.org/10.1155/2019/7428458

Research Article

Cascading Failures Analysis Considering Extreme Virus Propagation of Cyber-Physical Systems in Smart Grids

Tao Wang,[1,2] **Xiaoguang Wei**,[3] **Tao Huang**,[1,4] **Jun Wang**,[1,2] **Luis Valencia-Cabrera**,[5] **Zhennan Fan**,[1,2] **and Mario J. Pérez-Jiménez**[5]

[1]*School of Electrical Engineering and Electronic Information, Xihua University, China*
[2]*Key Laboratory of Fluid and Power Machinery, Ministry of Education, Xihua University, Chengdu 610039, China*
[3]*School of Electrical Engineering, Southwest Jiaotong University, China*
[4]*Department of Energy, Politecnico di Torino, Italy*
[5]*Research Group on Natural Computing, Department of Computer Science and Artificial Intelligence, University of Seville, Spain*

Correspondence should be addressed to Xiaoguang Wei; wei_xiaoguang@126.com and Tao Huang; tao.huang@polito.it

Received 3 November 2018; Revised 14 January 2019; Accepted 18 February 2019; Published 13 March 2019

Guest Editor: Riccardo Patriarca

Communication networks as smart infrastructure systems play an important role in smart girds to monitor, control, and manage the operation of electrical networks. However, due to the interdependencies between communication networks and electrical networks, once communication networks fail (or are attacked), the faults can be easily propagated to electrical networks which even lead to cascading blackout; therefore it is crucial to investigate the impacts of failures of communication networks on the operation of electrical networks. This paper focuses on cascading failures in interdependent systems from the perspective of cyber-physical security. In the interdependent fault propagation model, the complex network-based virus propagation model is used to describe virus infection in the scale-free and small-world topologically structured communication networks. Meanwhile, in the electrical network, dynamic power flow is employed to reproduce the behaviors of the electrical networks after a fault. In addition, two time windows, i.e., the virus infection cycle and the tripping time of overloaded branches, are considered to analyze the fault characteristics of both electrical branches and communication nodes along time under virus propagation. The proposed model is applied to the IEEE 118-bus system and the French grid coupled with different communication network structures. The results show that the scale-free communication network is more vulnerable to virus propagation in smart cyber-physical grids.

1. Introduction

The smart grid, as a modern electrical network (EN) infrastructure, can enhance the efficiency, reliability, and security of traditional ENs based on the advancement of cyber-physical systems [1–3]. In a smart grid, the monitoring, control, and management of the EN depend closely on the smart information and communication (cyber) network [4–6], which works such that the EN ensures not only its own secure operation but also reliable operation of the entire communication network. Meanwhile, when the EN fails (especially, through cascading failure), fault cross-propagation between the electrical and communication networks (ECNs), called interdependent network, occurs, which increases the complexity of fault propagation owing to interactions between the ECNs. For example, the Italian blackout of 2003 was triggered by effects of the ECN [7]. Therefore, exploring the propagation mechanism of interactive cascading failures [8] in an interdependent network has been receiving increasing attention.

To date, the connection between the different coupling modes between ECNs and the robustness/vulnerability of interdependent networks has been investigated widely [9–12]. Studies have demonstrated that the different types of links between ECNs greatly impact the robustness of the network. For example, [10] reveals the double-network link allocation

strategy is superior to single-network link allocation strategy. Therefore, reasonably allocating the interconnecting links between ECNs is vital for improving the robustness of interdependent networks. Accordingly, a few models (e.g., Petri nets) have been introduced to reveal the mechanism of interactions leading to catastrophic blackouts [13]. However, these works have been done merely from the perspective of the structure of the coupling of the ECNs.

Meanwhile, the physical and operational characteristics considering the interactions have been focused on as well. In [14], the impact of communication network vulnerability on power system operation was assessed considering both latency and communication interruptions. The data exchange model is introduced for modeling cascading failures in interdependent networks [15]. Reference [16] proposes a simulation platform to analyze the ECN vulnerability by considering the control strategy of power balance. Similarly, other simulations [17, 18] have been proposed to analyze the fault mechanism considering interactions between ECNs. Although these studies have included the interactions between the communication network and EN, their focus is only to study how to set up the simulation platform by considering both the communication network and the EN. Moreover, the operational characteristics are only studied from a steady state point of view.

In addition, as communication networks become increasingly smart and as smart grids are increasingly accessed using the Internet owing to advancement of the energy Internet [19, 20], cyber threats (e.g., virus propagation; hacking attacks) leading to interactive cascading failures should be focused on [21, 22]. For instance, the 2015 blackout in the Ukraine was a typical coordinated cyber-attack in which malicious code was employed to tamper with data and control the server of the monitoring system [23]. In the face of potential threats, measures to enhance information security of communication networks [24] and a few robust and efficient cyber infrastructures [25] have been proposed. For example, in Qinghai, China, to prevent viral infection of networks, an antivirus system was installed to manage the power dispatching data network. This system successfully detected and neutralized 3384 viruses in 2010-2012 [26]. It is manifest that there is a need to consider the virus propagation in the communication network although it is a low-probability event, as such an event can cause immense harm to the ECN owing to the subtlety of the virus and the high speed at which the network is infected by using advanced attack methods.

With this background, in our paper, we propose a framework to analyze the performance of the ECN by considering the interactions between two types of propagations: fault propagation in the EN and virus propagation in the communication network.

In the EN, cascading failures have been analyzed from the perspective of the overloaded mechanism [15, 27–29]. When a line fails, the power transmitted over the line will be redistributed in the network, and thus, a fault may cause increased flow in other branches and even overload them, leading to the fault propagation. However, those analyses are generally performed by through a steady state fashion. In our study, we improved the dynamic power flow method to redistribute loads and adjust unbalanced power in the network during fault propagation by introducing the primary frequency regulation and the equations of rotors of generators. Notably, we only consider high-voltage transmission networks as the study objects.

For the virus propagation, virus spread models [30, 31] with time delay have been developed based on the complex network theory (CNT) from the perspective of the topological structure of the communication network. Generally, the communication network mainly has two topical topological structures: scale-free and small-world networks. This paper focuses on investigating the impacts of two types of networks on electrical networks during virus propagation. In other words, we analyze which type of communication network is more vulnerable from the network-wise perspective, i.e., once viruses are propagated in a communication network, which type of communication network can cause more damage to the electrical network. Meanwhile, we further analyze that in a communication network, the vulnerability of communication nodes with different degree is revealed by investigating the number of fault branches and blackout level of coupled electrical networks.

In addition, it should be noted that the most modern malware, surely most malware is used in known attacks to power grids and industrial controls, limits its own effectiveness by prematurely destroying/disabling nodes and is not self-replicating. Furthermore, currently in a real-world communication network vertexes will not be homogeneous; thus they will not support most of self-propagating malicious code. However, in order to consider a low-probability but high consequence scenario, in this paper, we assume a random constant spread malicious code (called "virus" in this paper) with the following features to investigate the impact of extreme case of self-propagating virus on the power system from the network-wise perspective:

(1) the virus can block the communication between infected vertexes and the control center;

(2) the virus can self-propagate among homogeneous vertexes;

(3) a few infectious vertexes can be cured with the probability owing to the strengthening of security measures;

(4) the differences of security level of each node are not considered.

The remainder of this paper is organized as follows. Section 2 describes the interactions between the ECNs in the coupling relationships and topological structures. In Section 3, the virus propagation models with time delay and information exchange model in the communication network are introduced. The dynamic power flow method and the overload mechanism are established in Section 4. The cascading failures model considering the interactions and the corresponding simulation analysis are described in Sections 5 and 6, respectively. In Section 7, we further discuss the contribution of this paper and the external validity of the modeling. Finally, conclusions are given with possible future work in Section 8.

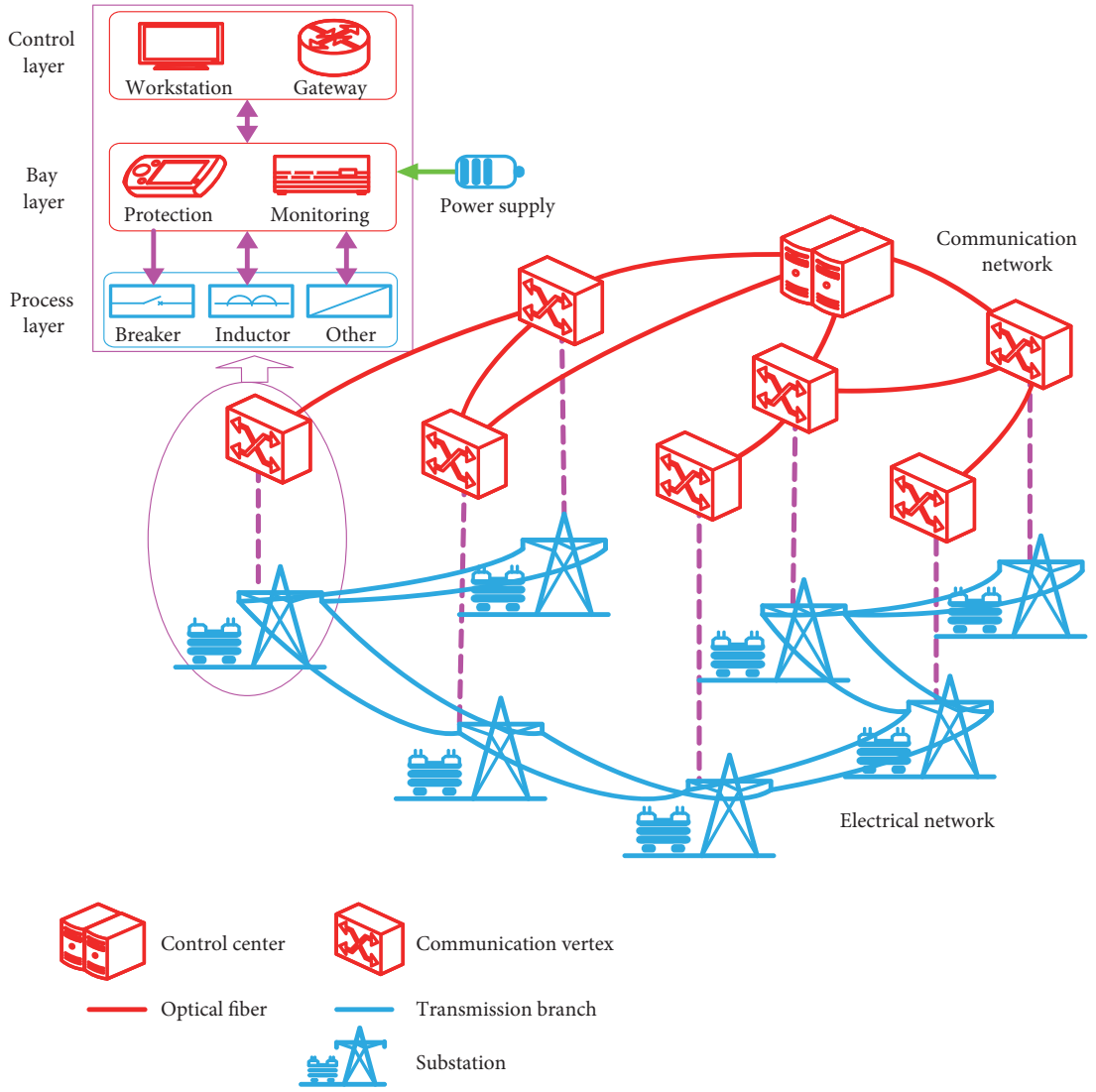

Figure 1: Diagram of ECN in smart grids.

2. Interaction between Electrical and Communication Networks in Smart Grid

2.1. Interdependent ECN in Smart Grids

ECN Spatial Model. The ECN in a smart grid is shown in Figure 1. The communication network, a hierarchical structure, is composed of optical fibers and synchronous digital hierarchies (SDHs), including control centers and communication vertexes [14, 32]. Generally, the substations (generators and loads) in the electrical network have the corresponding communication vertexes. The coupling between the substations and the communication vertexes is modeled by a smart communication module comprising three layers: process, bay, and control layers. Among the three layers, the bay layer is mainly responsible for accepting commands from the control layer to protect and monitor the electric network and realizing real-time interaction of information between the control and the process layers. The control layer is responsible for sending real-time messages from the electrical network to the control center as well as for accepting commands from the control center through the communication network.

ECN Operation Model. We analyze the ECN operation model from the perspective of energy flow. In an ECN, there are two types of energy flows: power flow and communication flow, as shown in Figure 2. In an EN, power flow changes with time via buses or lines. Conversely, because the communication vertexes transmit and receive messages at regular intervals, the communication flow is transmitted based on discrete time.

Communication Topology between Vertexes and Branches. Because there is a consistent one-to-one match between each communication vertex and each bus node, each transmission branch B_j has two related communication vertexes V_{m1} and V_{m2} during normal operation. In this paper, only V_{m1}

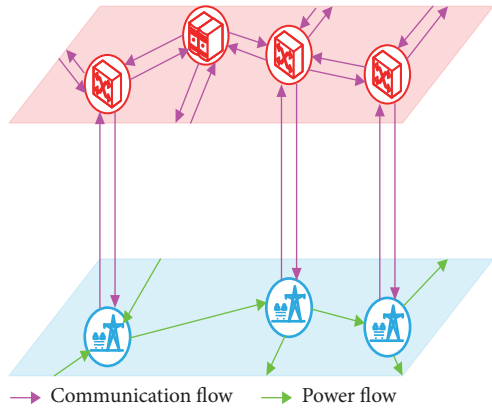

Figure 2: Information flows of electrical and communication networks in smart grids.

is considered for exchanging information packets with the control center [15].

2.2. Topological Structures of ECN

Electrical and Communication Network as Graphs. For simplifying analysis of the topological structures, we abstracted the ECN as graphs. The EN can be considered as a complex network with nodes and links. The buses, including generators, loads, and substations, can be viewed as nodes while transmission lines can be viewed as branches; therefore, the electrical network is represented as the graph $\mathbb{G}_E = (\mathbb{N}, \mathbb{B})$. The adjacent matrix $\boldsymbol{G}_E = (a_{ir})_{M_N \times M_N}$ is employed to define $\mathbb{G}_E$ as follows:

$$a_{ir} = \begin{cases} 1 & \exists N_i N_r = B_j \\ 0 & \neg \exists N_i N_r = B_j \end{cases} \quad (1)$$

where $N_i N_r = B_j$ represents that there is a branch B_j between nodes N_i and N_r.

Similarly, the optical fibers and SDHs of the communication network can be considered as edges and vertexes, respectively; therefore, the communication network is represented as the graph $\mathbb{G}_C = (\mathbb{V}, \mathbb{E})$. The adjacent matrix $\boldsymbol{G}_C = (a'_{mv})_{M_V \times M_V}$ is employed to define $\mathbb{G}_C$ as follows:

$$a'_{mv} = \begin{cases} 1 & \exists V_m V_v = E_a \\ 0 & \neg \exists V_m V_v = E_a \end{cases} \quad (2)$$

where $V_m V_v = E_a$ represents that there is an edge E_a between vertices V_m and V_v.

Because the buses are coupled with the corresponding communication vertexes by the communication module, which is represented as $\mathbb{L} = \{L_b \mid L_b = N_i V_m, i = m\}$, the ECN can be developed as an interdependent graph $\mathbb{G} = \mathbb{G}_E \cup \mathbb{G}_C = (\mathbb{N} \cup \mathbb{V}, \mathbb{B} \cup \mathbb{E} \cup \mathbb{L})$.

Topological Structure Analysis. We analyze the structural characteristics from the perspective of the CNT. Existing literature indicate that ENs have small-world networks [33–35], which demonstrates that ENs have a relatively small average shortest path but a very large cluster coefficient. Thus, the small-world electrical networks reveal that if a node (or branch) in the network fails, the adjacent and even nonadjacent nodes (or branches) could fail, leading to cascading failures. Meanwhile, ENs has scale-free characteristics, as determined by analyzing changes in the network structure and function when one or more nodes (or branches) are removed from the network, which shows the networks are highly vulnerable under deliberate attacks but robust under random attacks [28]. However, fault propagation mechanism of ENs studied from the perspective of pure topological structure is not comprehensive and should more focus on the physical and operational features.

In communication networks, generally, there are two types of topological networks: scale-free networks and small-world networks [15, 36, 37]. Communication networks with scale-free structures contain a few nodes with high degree, and they can be considered center nodes. Compared to the small-world networks, the distributions of degree of which are more uniform, scale-free networks have higher communication efficiency but are more vulnerable to deliberate attacks.

From the perspective of pure topological structures, compared to ENs, fault (or virus) propagation in communication networks is largely determined by its topological structure. That is, a fault node (or branch) only causes neighboring nodes to fail. Therefore, we employ the CNT to develop the virus propagation models (VPMs) based on the topological structures.

In summary, the EN and communication network in smart grids have two essential differences in terms of the interactions of cascading failures.

Features 1. From the perspective of time scales, the power flow is transmitted based on continuous time, while the communication flow is transmitted based on discrete time.

Features 2. From the perspective of topological structures, fault propagation in the communication networks depends more on the network structures. Compared with the communication networks, fault propagation in ENs depends more on physical and operational modes because ENs comply with operational rules, for example, Kirchhoff's law.

3. Virus Propagation and Information Exchange Models in Communication Networks

Before analyzing VPMs, we introduce the following topological concepts:

The degree k_{Vm} of V_m is the number of neighboring vertexes connected to V_m, as expressed by

$$k_{Vm} = \sum_{v=1}^{M_V} a'_{mv} \quad (3)$$

Degree distribution p(k) is the distribution function of the degrees. That is, when a vertex is randomly selected from the network, the probability that its degree is equal to k is p(k).

3.1. Virus Propagation Model Based on CNT. According to *Feature 1*, virus propagation in the communication network depends on the network structure; therefore, we employ the SI [38–40] and SIR [41, 42] models based on CNT to simulate virus propagation. In the SI model, the vertexes of the communication network are divided into two groups: susceptible set $\mathbb{S}$ and infectious set $\mathbb{I}$. In $\mathbb{S}$, the probability that a susceptible vertex contracts the virus from the infectious vertexes is β. Meanwhile, because the virus spends some time in destroying the functions of susceptible vertexes (e.g., tampering with data or instructions), the susceptible vertexes take time to get infected. Therefore, we introduce time delay (virus infection cycle) to develop the SI model as follows:

$$\begin{aligned} \frac{dS(t)}{dt} &= -\beta I(t-\tau_1) S(t-\tau_1) \\ \frac{dI(t)}{dt} &= \beta I(t-\tau_1) S(t-\tau_1) \end{aligned} \tag{4}$$

On the basis of the SI model, the SIR model considers that a few infectious vertexes can be cured with the probability owing to the strengthening of related antivirus measures (e.g., formatting operation). Thus, the infectious vertexes can obtain immunity in a certain virus removal cycle. Therefore, the vertexes add a group called removed set $\mathbb{R}$. The SIR model with time delay is given as

$$\begin{aligned} \frac{dS(t)}{dt} &= -\beta I(t-\tau_1) S(t-\tau_1) \\ \frac{dI(t)}{dt} &= \beta I(t-\tau_1) S(t-\tau_1) - \alpha I(t-\tau_2) \\ \frac{dR(t)}{dt} &= \alpha I(t-\tau_2) \end{aligned} \tag{5}$$

Because an infectious vertex only transmits the virus to its neighboring vertexes, the topological structure of the network greatly influences virus propagation. When the communication network is a small-world network, which can be regarded as a uniform network owing to the relatively uniform distribution of degree [37], the degree k_{Vm} of V_m is approximately equal to $\langle k \rangle$, and the SIR model can be presented as follows:

$$\begin{aligned} \frac{dS(t)}{dt} &= -\beta \langle k \rangle I(t-\tau_1) S(t-\tau_1) \\ \frac{dI(t)}{dt} &= \beta \langle k \rangle I(t-\tau_1) S(t-\tau_1) - \alpha I(t-\tau_2) \\ \frac{dR(t)}{dt} &= \alpha I(t-\tau_2) \end{aligned} \tag{6}$$

$$\begin{aligned} \frac{dS(t)}{dt} &= -\beta k S_k(t-\tau_1) \frac{\sum_k kp(k) I_k(t-\tau_1)}{\langle k \rangle} \\ \frac{dI(t)}{dt} &= \beta k S_k(t-\tau_1) \frac{\sum_k kp(k) I_k(t-\tau_1)}{\langle k \rangle} \\ &\quad - \alpha I(t-\tau_2) \\ \frac{dR(t)}{dt} &= \alpha I(t-\tau_2) \end{aligned} \tag{7}$$

When the communication network is a scale-free network, the vertexes have different damage levels from the perspective of virus propagation because the distribution of degree follows a power law. That is, the greater the k_{Vm} of V_m, the more serious it is for the V_m to spread or contract the virus to more vertexes. The SIR model can be expressed as (7) in terms of the vertex degree [43, 44].

Generally, in the SI and SIR models, virus propagation is faster in scale-free networks owing to the power law distribution. In addition, by comparing SI and SIR models, once virus propagation occurs in the communication network, we can investigate whether the related antivirus measures with time delay can play an important role to prevent the fault from spreading across the EN.

3.2. Information Exchange Model in Communication Network. In the smart grid, the communication vertexes send operational data (parameters) associated with branches to the control center and receive commands from the control center step-by-step through the communication network in the form of information packets. At every step, the same information packets can be received and sent only by each communication vertex. Before constructing the information exchange model, three simplifications are made as follows.

(1) The communication blocks of vertexes (or edges) are not considered in process of the information transfer when the vertexes work orderly. That is, the capacity of the vertexes is adequate to exchange/handle the information packets.

(2) Because the vertexes send and receive information packets at intervals of 0.833 ms [45], the time required for information exchange between the vertexes and control center can be ignored because it is very small compared to the time required for fault propagation in the EN.

(3) Because we focus on the interactions between the ECNs, the methods of gathering and dealing with the information (such as the measuring units, transmission channels and protocols, encryption and decryption algorithms, etc.) are not considered.

Based on the above simplifications, the information exchange model is constructed based on the structure of the communication network.

Communication Rules between Target Vertex and Control Center. The vertexes abide by the rule of first-in-first-out to send out information packets to avoid exchange of the information packets to be in the same edge. At first, the target vertex produces information packets. Then, the information packets are sent to all its neighbor vertexes. If the control center is one of the neighbor vertexes, the information

transfer ends; otherwise, all neighbor vertexes, acting as target vertexes, continue to send the information packets to their corresponding neighbor vertexes until the information packets are sent to the control center. In the above process, the information packets are transmitted successfully between the target vertex and control center if a path exists between them in the communication network.

4. Dynamic Power Flow and Overload Mechanism Models in Electrical Networks

4.1. Dynamic Power Flow in Electrical Networks. To redistribute power flow during disturbances, we employ primary frequency regulation [46, 47] and rotor equation [48] to model the dynamic power flow method.

System Frequency Characteristics. We employ primary frequency regulation to adjust the power flow. The characteristics of load and generation frequency are given by (8) and (9), respectively.

$$\Delta P_X = K_X \Delta f \tag{8}$$

$$\Delta P_W = K_W \Delta f \tag{9}$$

K_X and K_W are calculated as follows:

$$K_X = \frac{\sum_{q=1}^{N_X} \left(K_{Rq} \cdot P_{Rrq}\right)}{\sum_{q=1}^{N_X} P_{Rrq}} \tag{10}$$

$$K_W = \frac{\sum_{c=1}^{N_W} \left(K_{Wc} \cdot P_{Wrc}\right)}{\sum_{c=1}^{N_W} P_{Wrc}} \tag{11}$$

Unbalanced Power Redistribution. To redistribute the unbalanced power P_{un} due to disturbances of the system, we first calculate the change in system frequency by using the primary frequency regulation and the rotor equation.

$$T_J \frac{d\Delta\omega}{dt} = P_{un} - K_E \cdot \Delta\omega(t) \tag{12}$$

In (12), P_{un} is calculated as follows:

$$P_{un} = \sum_{c=1}^{M_W} P_{Wc} - \sum_{c=1}^{M_X} P_{Xq} \tag{13}$$

When $P_{un} < 0$, we consider the characteristics of load and the generation frequency to adjust the system frequency:

$$K_E = K_X + K_W \tag{14}$$

When $P_{un} > 0$, we consider only the generation frequency characteristic:

$$K_E = K_W \tag{15}$$

By using (8)-(15), the changes in every generator and load can be expressed as follows:

$$\Delta P_{Xq} = K_{Xq} \cdot \Delta\omega(t) \tag{16}$$

$$\Delta P_{Wc} = K_{Wc} \cdot \Delta\omega(t) \tag{17}$$

Then, we employ the P-Q power flow to calculate the power flows of each bus ($q = c = i$) as follows:

$$\begin{aligned} P_i &= -\Delta P_{Wq} + \Delta P_{Xc} \\ &\quad + \nu_i \sum_{u=1}^{M_N} \nu_u \left(G_{iu} \cos\theta_{iu} + B_{iu} \sin\theta_{iu}\right) \\ &= \left(-K_{Wq} + K_{Xc}\right) \Delta\omega \\ &\quad + \nu_i \sum_{u=1}^{M_N} \nu_u \left(G_{iu} \cos\theta_{iu} + B_{iu} \sin\theta_{iu}\right) \end{aligned} \tag{18}$$

$$Q_i = \nu_i \sum_{u=1}^{M_N} \nu_u \left(G_{iu} \sin\theta_{iu} - B_{iu} \cos\theta_{iu}\right) \tag{19}$$

Dynamic Power Flow Method. When branches fault during fault propagation in the network, the dynamic power flow can be calculated in Algorithm 1.

4.2. Overload Mechanism of Electrical Networks. In this paper, cascading failures in the EN are analyzed from the perspective of the overload mechanism. When one or more lines are cut off, the other lines are overloaded owing to the redistribution of power flow in the EN [27, 28]. When a branch is overloaded, the larger the power flow over the branch, the shorter is the operational time for which the branch is permitted to continue working [15]. As most of other studies [15, 49], in this paper, we assume that during the fault propagation, the control center tries to maintain the secure operation of the EN and lower the load shedding amount, thus the control strategy includes which branches to trip, how to adjust the generators output, as well as to shed which load of how many percentages, etc. Therefore, for some of the branches, the tripping command has to come from the control center. Of course, for some of the faulted lines, the tripping signal should be issued by a local protection unit. However, to simplify the process, we simply assume that the tripping command comes from the control center. Thus, under thus simplification, when the corresponding communication vertexes send information about overloading to the control center via the communication network, the control center must quickly send trip commands to the target vertexes. We employ the inverse-time overcorrect protection scheme [15, 49] to calculate the overloaded operational time.

$$t_{B_j} = \frac{\kappa}{\left|I_{B_j}/\bar{I}_{B_j}\right|^{\sigma} - 1} \tag{20}$$

If the data exchange between the target vertex and control center to trip the branch B_j is completed within t_{Bj}, the control is successful; otherwise, the control is unsuccessful.

5. Interactive Cascading Failure Model

A diagram of cascading failures considering the interactions between the ECN is shown in Figure 3. During the cascading

Input: Electrical network information
Output: Power flows of branches, frequency violation
Step 1: Unbalanced power: Employ Equation (13) to calculate the unbalanced power P_{un} of the network.
Step 2: System frequency characteristic: **IF** $P_{un} < 0$, employ Equation (14) to calculate K_S and go to the next step; **ELSE**, **IF** $P_{un} > 0$, employ Equation (15) to calculate K_S and go to the next step; **ELSE**, go to **Step 4**.
Step 3: Frequency calculation: Calculate variation $\Delta f(t)$ of frequency of the network by Equation (12) solved using improved Euler method ($\Delta t = 0.01$ s).
Step 4: Generator frequency detection: **IF** $\Delta f(t)$ is beyond limits of generator i, cut off generator i and return to **Step 3**; **ELSE**, go to the next step.
Step 5: Frequency violation: **IF** $\Delta f(t)$ is beyond limits the network, end the algorithm and send warnings of of instability; **ELSE**, go to the next step.
Step 6: Power flow calculation: Employ the P-Q power flow to calculate the power flows of every branch.

Algorithm 1: Dynamic power flow method.

failures in the EN, if branch B_j is overloaded, according to the control strategy, B_j generates fault information packets, and the corresponding communication vertexes then send these packets to the control center via the communication network. Thereafter, the control center sends the commands back to B_j within t_{B_j}.

In addition, when the virus spreads through the communication network, the infectious vertex V_l will lose the function of information exchange and connectivity a'_{ml} with its neighbor vertexes, according to

$$a'_{ml} = 0 \quad (\mathrm{m} = 1, 2, \ldots, \mathrm{M_V}) \tag{21}$$

Meanwhile, the virus will cause branches to trip or lead to an outage directly or indirectly because the infectious vertexes lose the function of information exchange. Accordingly, there are four types of fault branches.

Type 1. The branch is forced to trip because the corresponding communications get infected, also called forced outage branches $\mathbb{B}_{FO}$.

Type 2. The branch is tripped properly because the control center successfully sends commands to the corresponding vertexes based on the received overload information and control strategy with t_{B_j}, also called overload tripping branches $\mathbb{B}_{OT}$.

Type 3. The branch is damaged irreparably owing to control failures via the communication networks, leading to overload operational time exceeding t_{Bj}, also called irreparable fault branches $\mathbb{B}_{IF}$.

Type 4. The branch undergoes forced outage owing to network splitting, also called network splitting branches $\mathbb{B}_{NS}$.

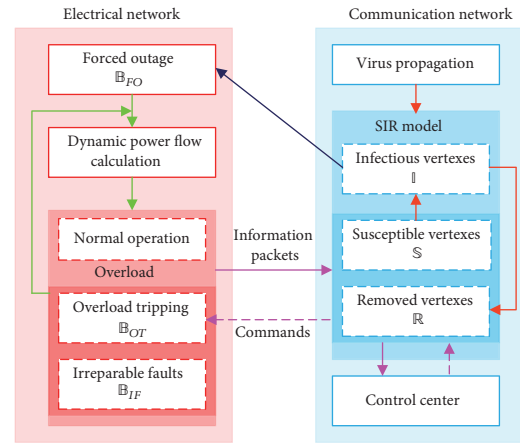

Figure 3: Cascading failures considering interactions between ECNs.

Based on the above analysis, cascading failure considering the interactions between the ECNs is modeled in Algorithm 2.

6. Case Study

The proposed model was applied to the IEEE 118-bus system and the French grid [50]. The small-world and scale-free networks were adopted to represent the respective communication networks. The computational work was performed in MATLAB running on a laptop. The laptop (Compaq, v3646TU) was equipped with an Intel® Core™ 2 Duo CPU T7250@2.00 GHz, 2.00 GB RAM, and 64-bit Windows 7 operating system.

Input: Electrical network information and parameters, communication network information and parameters, η, $\mathbb{I}$, β, α, τ_1
Output: ϑ, $\mathbb{B}_{FO}$, $\mathbb{B}_{OT}$, $\mathbb{B}_{IF}$, $\mathbb{B}_{NS}$
Step 1: Initialization: t = 0 s, $\vartheta = 0$, $\mathbb{B}_{FO} = \emptyset$, $\mathbb{B}_{OT} = \emptyset$, $\mathbb{B}_{IF} = \emptyset$, $\mathbb{B}_{NS} = \emptyset$, $\mathbb{B}_O = \emptyset$, $\mathbb{S} = \emptyset$, $\mathbb{R} = \emptyset$, $\mathbb{R}' = \emptyset$ and $\mathbb{I}' = \emptyset$.
Step 2: WHILE t<η
Electrical network:
Step 3: Forced branch outage: **IF** the corresponding vertexes coupled with the branch B_j (j = $1, 2, \ldots, M_B$) are in $\mathbb{I}$, add the branch B_j to $\mathbb{B}_{FO}$ and trip it.
Step 4: Overloaded branch tripping: **IF** the overload operation time of $B_x(B_x \in \mathbb{B}_O)$(x = $1, 2, \ldots, M_O$) in t_{Bx} = t, and the fault packages between the corresponding vertexes and control center are exchanged successfully, add B_x to $\mathbb{B}_{OT}$, and delete B_x from $\mathbb{B}_O$; **ELSE**, **IF** t_{Bx} > t, add B_x to $\mathbb{B}_{IF}$, and delete B_x from $\mathbb{B}_O$
Step 5: Network splitting: Detect and split the electrical network. **IF** there exists the forced outage branch B_z (z = $1, 2, \ldots, M_{NS}$) due to the splitting, add B_z to $\mathbb{B}_{NS}$.
Step 6: Network operational status**:** Calculate the power flow over B_j (j = $1, 2, \ldots, M_B$). **IF** B_j is overloaded, calculate t_{Bj} of B_j by Equation (19), and add B_j to $\mathbb{B}_O$.
Communication network:
Step 8: Infectious vertexes detection: **IF** the infection time of the candidate vertex V_k (k = $1, 2, \ldots, M_{I'}$) in $\mathbb{I}'$ is equal to t, add V_k to $\mathbb{I}$ and delete it from $\mathbb{I}'$.
Step 10: Removal of vertex detection: **IF** the removal time of the candidate vertex V_ω (w = $1, 2, \ldots, M_{R'}$) in $\mathbb{R}'$ is equal to t, add V_w to $\mathbb{R}$, and delete it from $\mathbb{R}'$.
Step 7: Virus propagation: The susceptible vertex V_g (g = $1, 2, \ldots, M_S$) contracts the virus with probability β according to Equation (6). **IF** V_g gets infected, delete V_g from $\mathbb{S}$, add V_g to $\mathbb{I}'$, and label its infectious time t + τ_1.
Step 9: Vertex immunization: The infected vertex V_l (l = $1, 2, \ldots, M_I$) is immunized with the probability α according to Equation (6). **IF** V_l obtains immunity, delete V_l from $\mathbb{I}$, add V_l to $\mathbb{R}'$, and label its immunity time t + τ_2.
Step11: t = t + Δt; **END WHILE**.

Algorithm 2: Cascading failure model considering interactions between ECNs (SIR model as an example).

6.1. IEEE 118-Bus System. We randomly chose the communication vertexes as the initial infectious vertexes and then performed 1000 cascading events to investigate load shedding and number of instances of the four types of fault branches (M_{IF}, M_{OT}, M_{FO}, and M_{NS}) based on the different VPMs and topological structures of the communication network with the parameters $\Delta t = 0.01$ s, $\tau_1 = \tau_2 = 5s$, $\alpha = \beta = 0.3$, $\kappa = 7$ and $\sigma = 1.5$. The averaged results are shown in Figure 4 and listed in Table 1.

Figure 4 shows that the load shedding changes with the passage of time based on the different topological structures of the communication networks and the SI model. Owing to space limits, the SIR-model-based load shedding is not given herein. In Figure 4, the propagation time of interactive cascading failures depends on the virus propagation time τ_1, and the load shedding is the maximum when the propagation time is approximately 10s. Compared with the small-world communication network, the propagation time of interactive cascading failures is longer in the scale-free communication network. Moreover, coupling with the scale-free communication network, the fault branches of the EN result in irreparable faults (M_{IF} = 3.415) with higher probability than that (M_{IF} = 0.245) in the case of coupling with the small-world communication network, as summarized in Table 1. Therefore, the coupling of EN with the scale-free communication network is affected more severely as the propagation time increases because the connectivity between vertexes often depends on a few hub vertexes (i.e., high-degree vertexes), and the exchange of information packets becomes difficult, leading to network paralysis once a few hub vertexes are infected.

A comparison of the SI and the SIR models shows that different VPMs have very small impacts on fault propagation

Table 1: Average numbers of four types of fault branches.

VPMs	Structures	M_{FO}	M_{IF}	M_{OT}	M_{NS}
SI	**SW**	148.164	0.245	14.589	9.1554
	SF	142.977	3.415	14.643	10.1554
SIR	**SW**	148.222	0.139	14.658	9.336
	SF	143.104	1.371	16.588	10.064

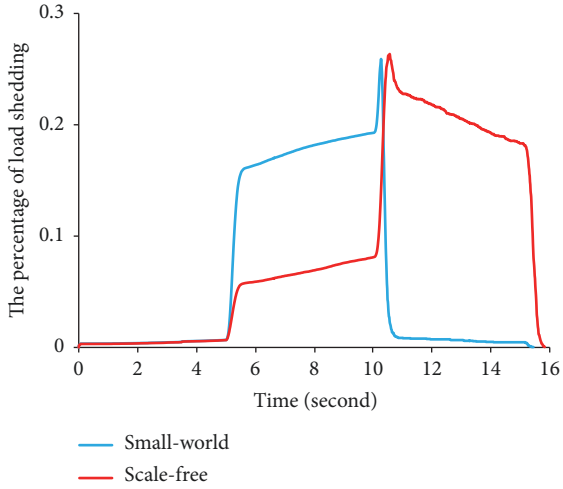

Figure 4: Load shedding of IEEE 118-bus system over time based on SI model.

in the EN, which indicates that once fault propagation occurs in the EN, the related antivirus measures with time delay can barely prevent the fault from spreading across the EN. However, the number of fault branches with irreparable faults can be reduced, especially in the case of coupling with the scale-free communication network. This is because the immune vertexes treated with the antivirus recover their function of data exchange, and a few overloaded branches can receive trip commands from the control center in a timely manner, thus avoiding irreparable faults.

Furthermore, we analyze the interactive cascading failures by selecting different initial infectious vertexes. We used the SI model as an example. Because the degree distributions of the small-world communication network are known, we take the scale-free network as the basis to select the high-degree (vertexes 115 and 116) and small-degree (vertexes 4 and 8) vertexes as the initial infectious vertexes. Figures 5 and 6 show the total and real-time load shedding changes with the passage of time for different virus propagation times τ_1= 2 s, 5 s, and 8 s. The initial vertexes have small impacts on fault propagation in the EN owing to the known degree distribution. However, in case of the coupling of the EN with the scale-free communication network, the initial vertexes greatly impact fault propagation. Compared to the small-world communication network, when the initial vertexes are high-degree vertexes in the scale-free communication network, the propagation time is obviously shorter, which demonstrates the hub can rapidly spread the virus, leading to rapid collapse of the EN. By contrast, the propagation time is longer when the initial vertexes are the low-degree vertexes, and when the load shedding peaks, as shown in Figure 6, the interactive cascading failures continue to spread, which indicates virus propagation times are longer than fault propagation times. That is, when fault propagation has stopped, virus propagation continues.

6.2. French Grid. A real French grid with 1951 nodes and 2956 branches was employed to simulate the interactive model. Owing to computational complexity, we only choose the high-degree vertexes as initial infectious vertexes considering the topological structures of the communication network with the parameters $\Delta t = 0.01$ s, $\tau_1 = \tau_2 = 2$s, $\alpha = \beta = 0.3$, $\kappa = 7$, and $\sigma = 1.5$. Figure 7 shows that the total and real-time load shedding of system changes with the passage of time. Compared to the small-world communication network, the propagation times are longer in the case of EN coupled with scale-free communication network, but the load shedding peaks at approximately 8.3 s under both topological structures.

Furthermore, we investigated the numbers of the three types of fault branches (M_{IF}, M_{OT}, and M_{FO}) at different moments, as shown in Figures 8(a) and 8(b). Between 6 s and 7 s, the fault propagation is at its height, which indicates that the numbers of infectious vertexes and forced outage branches $\mathbb{B}_{FO}$ are the highest, leading to rapid collapse of the EN and surging load loss. In addition, in the fault propagation process in the EN, the fault branches with irreparable faults are not found when the EN is coupled with the small-world communication network. By contrast, there are many fault branches of this type at different moments in the case of EN coupled with the scale-free communication network. Therefore, when the communication network is scale-free, it is more vulnerable which cannot effectively resist the virus propagation leading to the more severe damage to the EN.

The conclusions obtained from these two cases are summed up in Table 2. In practice, when ENs are faced with hacker attacks, because the attackers find it relatively difficult to obtain complete information about the communication networks, such as topological structures, their attacks are random to some extent, which means scale-free communication networks are more appropriate for the ENs [10, 30, 31]. However, when ENs are faced with the threat of a cyber virus, the virus must be cleared promptly. Once the virus spreads, regardless of whether the initial infectious vertexes are selected randomly or deliberately, the infection will lead to a severe damage in the scale-free communication networks. Therefore, due to the propagation features of the scale-free communication networks, the simulation results show that software engineers should strengthen more the software

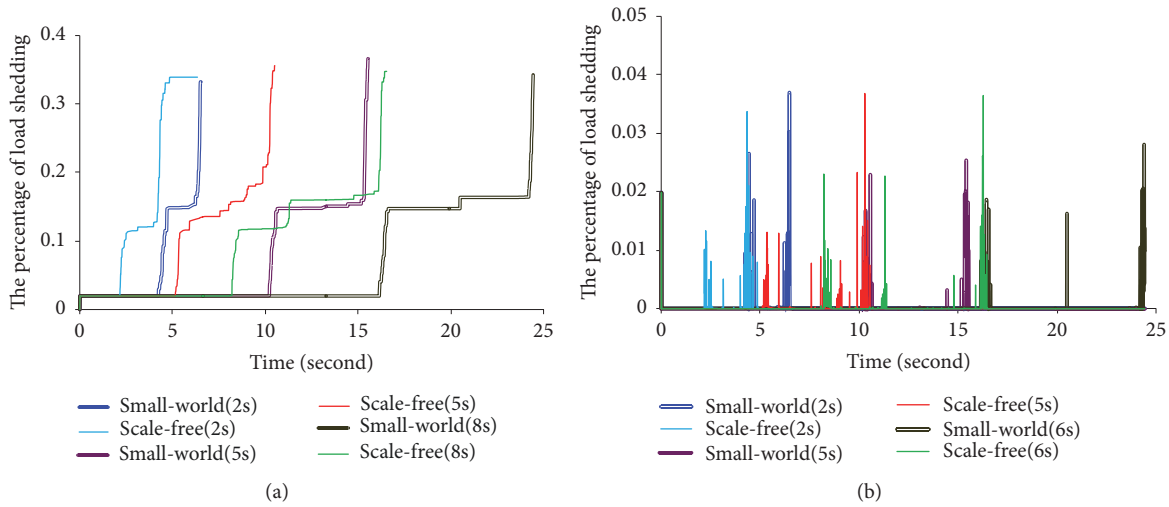

FIGURE 5: Load shedding of IEEE 118-bus system over time in the case of high-degree initial infectious vertexes. (a) Total load shedding over time; (b) real-time load shedding.

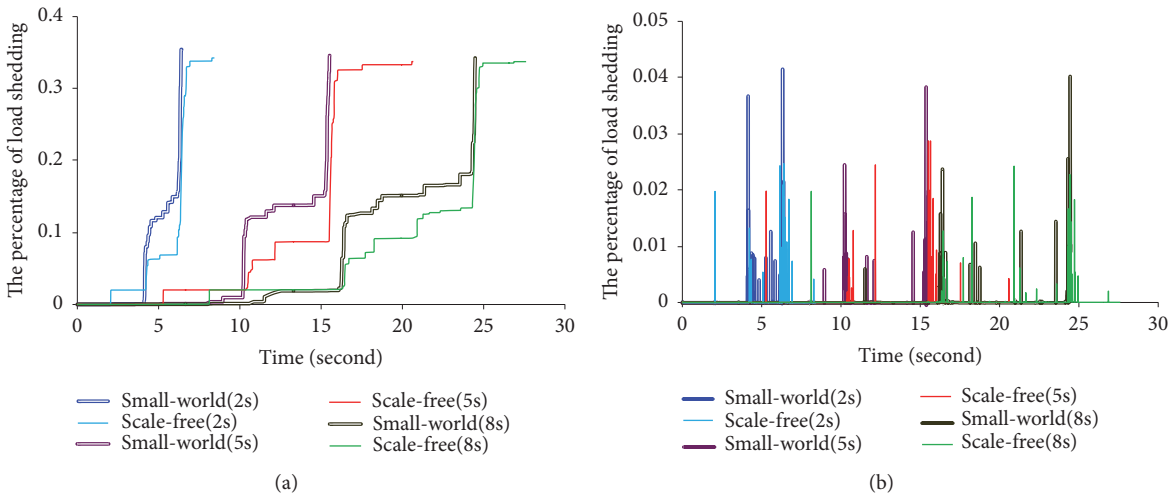

FIGURE 6: Load shedding of IEEE 118-bus system over time with low-degree initial infectious vertexes. (a) Total load shedding over time; (b) real-time load shedding.

protections in the scale-free communication networks by means of more frequent update of the firewalls and antivirus software, strategies of automatic system restoration, etc.

7. Discussion

In this paper, we extend the state of the art for the study of the integrated communication network and electrical network. Compared with other literature, the main contributions of our paper are as follows:

We propose an interdependent fault propagation model which holistically considers the extreme virus propagation in the communication network to reveal the vulnerability of electrical network coupled with different communication network structures at the first time.

In the fault propagation model, to better reproduce the ex-post behavior of the electrical networks, we extended the dynamic power flow by including the primary frequency regulation and the equations of rotors of generators.

To solve the issue of different time frames in the interdependent system, we adopt two time windows, i.e., the virus infection cycle of nodes and tripping time of overloaded branches during fault propagation to analyze the fault mechanism of both electrical branches and communication nodes along time.

It should be noted that even though the electrical network and communication network are both presented as graphs to conveniently describe their interdependent topological relationship in this paper, the modeling approach captured most of the relative features of the two networks.

For the electrical network, besides the commonly considered steady state physical and operational rules, we also adopt the rotor equation and system frequency to consider simple system dynamics in order to present the interactions between

Table 2: Comparison of propagation times between SW and SF networks.

Objects	Types of propagation	Initial factious vertexes	
		High-degree	Low-Degree
ECN	Interactive	SW>SF	SW<SF
Electrical network	Fault	SW=SF	SW=SF
Communication Network	Virus	SW>SF	SW<SF

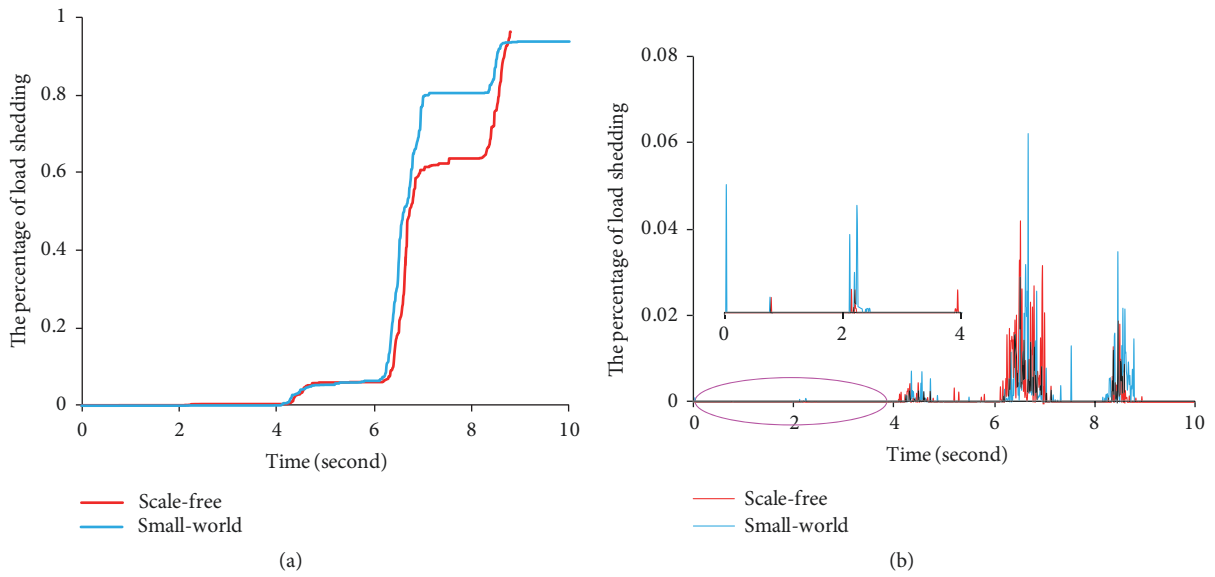

Figure 7: Load shedding of IEEE 118-bus system over time based on SIR model. (a) Total load shedding over time; (b) real-time load shedding.

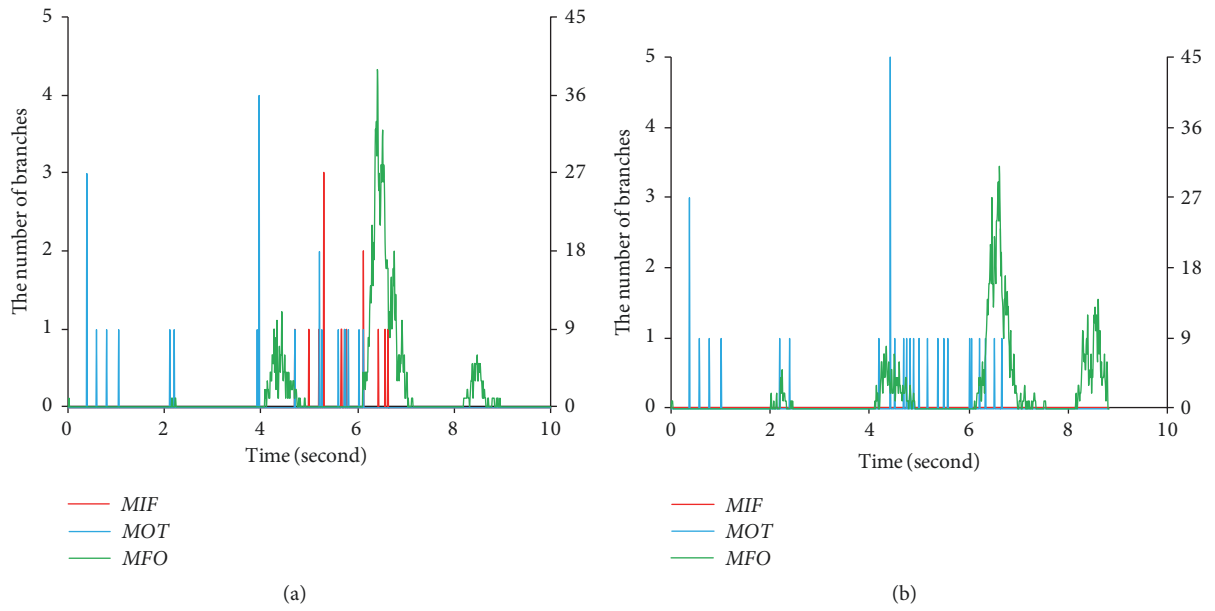

Figure 8: Numbers of different types of fault branches over time based on SIR model. (a) Scale-free network; (b) small-world network.

the electrical network and the communication network. As for the communication networks, we assume that the security level of each node is the same in terms of the infected rate. By contrast, in reality, the probability of the communication nodes got infected may vary for different nodes. However, the assumption made in our paper does not change the essence of the analysis and results in terms of evaluating which topology of communication network would have higher impacts on the electrical network during cyber-attacks.

8. Conclusions

The cyber-physical security of power systems is attracting increasing attention, especially after more and more evidences show that failures or attacks happening in the cyber system can greatly destroy the secure operation of power systems and bring tremendous consequences. To investigate the possible consequences, we propose an approximate interactive model to study cascading failures in ENs caused by virus in communication networks via two types of propagation. Our simulation on a standard study case, i.e., IEEE 118-bus system, and a realistic network, i.e., French grid, shows that the structure of the communication network has decisive impacts on the ECN in terms of the propagation time of cascading failures, loading shedding, number of faulted branches, etc. However, due to the simplification of the communication network and the virus propagation mechanism, the model can still be refined. In addition, the analysis is only focused on the overload of the system which may limit the results to part of behaviors of the EN.

Owing to the complexity of the propagation mechanism of interactive cascading failures, future work in this field will focus on considering more factors, such as data transmission delay, to simulate interactive cascading failures. Meanwhile, we also can investigate the impacts of differences of virus infection of nodes on interdependent fault propagation for electrical and communication networks. In addition, we can also analyze other aspects of the integrated CPS system, such as reliability, resilience, etc., under the virus propagation, to provide other dimensions for understanding the CPS.

Nomenclature

ECN: Electrical and communication network
SDH: Synchronous digital hierarchy
CNT: Complex network theory
VPM: Virus propagation model
SM: Small-world
SF: Scale-free
EN: Electrical network.

Sets (Note That $|\cdot|$ Represents the Dimension of a Set)

$\mathbb{N}$: Set of nodes (i.e., buses) in an electrical network, $\mathbb{N} = \{\cdots, N_i, \cdots\}$, $|\mathbb{N}| = M_N$
$\mathbb{W}$: Set of nodes with generators, $\mathbb{W} = \{\cdots, W_c, \cdots\} \subseteq \mathbb{N}$, $|\mathbb{W}| = M_W$
$\mathbb{X}$: Set of nodes with loads, $\mathbb{X} = \{\cdots, X_q, \cdots\} \subseteq \mathbb{N}$, $|\mathbb{X}| = M_X$
$\mathbb{B}$: Set of branches (i.e., lines) in an electrical network, $\mathbb{B} = \{\cdots, B_j, \cdots\}$, $\mathrm{N_i N_r} = \mathrm{B_j}$, $|\mathbb{B}| = M_B$
$\mathbb{G}_E$: Electrical network, $\mathbb{G}_E = (\mathbb{N}, \mathbb{B})$
$\mathbb{V}$: Set of vertexes (i.e., optical fibers) in a communication network, $\mathbb{V} = \{\cdots, V_m, \cdots\}$, $|\mathbb{V}| = M_V$
$\mathbb{E}$: Set of edges (i.e., SDHs) in a communication network, $\mathbb{E} = \{\cdots, E_a, \cdots\}$, $\mathrm{V_m V_v} = \mathrm{E_a}$, $|\mathbb{E}| = M_E$
$\mathbb{G}_C$: Communication network, $\mathbb{G}_C = (\mathbb{V}, \mathbb{E})$
$\mathbb{L}$: Set of links which present the couples between electrical network and communication network, $\mathbb{L} = \{\cdots, L_b, \cdots\}$, $L_b = N_i V_m$, $i = m$, $|\mathbb{L}| = M_L$
$\mathbb{G}$: Electrical and communication network, $\mathbb{G} = \mathbb{G}_E \cup \mathbb{G}_C$
$\mathbb{S}$: Set of susceptible vertexes, $\mathbb{S} = \{\cdots, V_g, \cdots\} \subseteq \mathbb{V}$, $|\mathbb{S}| = M_S$
$\mathbb{I}$: Set of infectious vertexes, $\mathbb{I} = \{\cdots, V_l, \cdots\} \subseteq \mathbb{V}$, $|\mathbb{I}| = M_I$
$\mathbb{I}'$: Set of candidate infectious vertexes, $\mathbb{I}' = \{\cdots, V_k, \cdots\} \subseteq \mathbb{V}$, $|\mathbb{I}'| = M_{I'}$
$\mathbb{R}$: Set of removed vertexes, $\mathbb{R} = \{\cdots, V_h, \cdots\} \subseteq \mathbb{V}$, $|\mathbb{R}| = M_R$
$\mathbb{R}'$: Set of candidate removed vertexes, $\mathbb{R}' = \{\cdots, V_w, \cdots\} \subseteq \mathbb{V}$, $|\mathbb{R}'| = M_{R'}$
$\mathbb{B}_{IF}$: Set of branches with irreparable faults due to the control failures, $\mathbb{B}_{IF} = \{\cdots, B_e, \cdots\} \subseteq \mathbb{B}$, $|\mathbb{B}_{IF}| = M_{IF}$
$\mathbb{B}_{OT}$: Set of fault branches with overload tripping due to the control successes, $\mathbb{B}_{OT} = \{\cdots, B_g, \cdots\} \subseteq \mathbb{B}$, $|\mathbb{B}_{OT}| = M_{OT}$
$\mathbb{B}_{FO}$: Set of branches with forced outage due to the corresponding communication vertexes get infected, $\mathbb{B}_{FO} = \{\cdots, B_y, \cdots\} \subseteq \mathbb{B}$, $|\mathbb{B}_{FO}| = M_{FO}$
$\mathbb{B}_{NS}$: Set of branches with forced outage due to the network splitting, $\mathbb{B}_{NS} = \{\cdots, B_z, \cdots\} \subseteq \mathbb{B}$, $|\mathbb{B}_{NS}| = M_{NS}$
$\mathbb{B}_O$: Set of overloaded branches, $\mathbb{B}_O = \{\cdots, B_x, \cdots\} \subseteq \mathbb{B}$, $|\mathbb{B}_O| = M_O$.

Constants

a_{ir}: The branch between $\mathrm{N_i}$ and $\mathrm{N_r}$
a'_{mv}: The edge between $\mathrm{V_m}$ and $\mathrm{V_v}$
$\mathrm{P_{Wrc}}$: Power rating of generator c
$\mathrm{P_{Rrq}}$: Power rating of load q
$\mathrm{K_{Wc}}$: cth generator unit power regulation
$\mathrm{K_W}$: Equivalent generator unit power regulation
$\mathrm{K_{Xq}}$: qth load frequency regulation
$\mathrm{K_X}$: Equivalent load frequency regulation
$\mathrm{K_E}$: System unit power regulation
$\mathrm{T_J}$: Equivalent Inertia time constant
$\mathrm{T_{Jc}}$: Inertia time constant of generator c

k_{Vm}: Degree of vertex m
p(k): Degree distribution
κ: Proportional coefficient of inverse-time overcurrent protection
σ: Power coefficient of inverse-time overcurrent protection
$\bar{I}_{Bj}$: Current limit of branch B_j.

Variables

t: Time / clock
t_{Bj}: Overloaded operational time of branch B_j
η: Simulation time
$\cdot(t)$: Value / set of a variable at time t
Δt: Time step
$\cdot_k$: Value / set of vertex(es) with k degrees
P_{un}: System unbalanced power
Δf: Frequency offset
ΔP_W: Changes of power of all generators
ΔP_{Wc}: Changes of power of generator c
ΔP_X: Changes of power of all loads
ΔP_{Xq}: Changes of power of load q
P_{Xq}: Power of load q
I_{Bj}: Current over branch B_j
P_i: Injection active power of node i
Q_i: Injection reactive power of node i
B_{iu}: Equivalent susceptance between nodes i and u
G_{iu}: Equivalent conductance between nodes i and u
θ_{iu}: Voltage phase angle difference between nodes i and u
v_i: Voltage of node i
$\Delta\omega$: Changes of angular acceleration of equivalent generator
ϑ: The percentage of load shedding
S: Percentage of susceptible vertexes, $S = M_S/M_V$
I: Percentage of infectious vertexes, $I = M_I/M_V$
R: Percentage of removed vertexes, $R = M_R/M_V$
β: Infection rate from susceptible vertex to infectious vertex
α: Recovery rate from infectious vertex to removed vertex
τ_1: Virus infection cycle
τ_2: Virus removal cycle.

Matrix

$\boldsymbol{G}_E$: Connectivity of the graph $\mathbb{G}_E$, $\mathbf{G}_E = (a_{ir})_{M_N \times M_N}$
$\boldsymbol{G}_C$: Connectivity of the graph $\mathbb{G}_C$, $\mathbf{G}_C = (a'_{mv})_{M_V \times M_V}$.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

All authors declare that they have no conflicts of interest.

Acknowledgments

This research was partially funded by grants from the National Natural Science Foundation of China (51877181, 61703345, and 51607146), the Key Fund Project of the Sichuan Provincial Education Department (18ZA0459), the Key Scientific Research Fund Project of Xihua University (Z17108), and the Young Scholars Reserve Talents Support Project of Xihua University.

References

[1] C. Vellaithurai, A. Srivastava, S. Zonouz, and R. Berthier, "CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 566–575, 2015.

[2] M. M. Rana, L. Li, S. W. Su, and W. Xiang, "Concensus based smart grid state estimation algorithm," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3368–3375, 2018.

[3] M. M. Rana and L. Li, "An overview of distributed microgrid state estimation and control for smart grids," *Sensors*, vol. 15, no. 2, pp. 4302–4325, 2015.

[4] D. T. Nguyen, Y. Shen, and M. T. Thai, "Detecting critical nodes in interdependent power networks for vulnerability assessment," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 151–159, 2013.

[5] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control of microgrids," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 2, pp. 602–609, 2018.

[6] J. Le, C. Wang, W. Zhou, Y. Liu, and W. Cai, "A novel PLC channel modeling method and channel characteristic analysis of a smart distribution grid," *Protection and Control of Modern Power Systems*, vol. 2, no. 2, pp. 146–158, 2017.

[7] A. Berizzi, "The Italian 2003 blackout," in *Proceedings of the 2004 IEEE Power Engineering Society General Meeting*, pp. 1673–1679, Denver, CO, USA, June 2004.

[8] Q. Sun, L. Shi, Y. Ni, D. Si, and J. Zhu, "An enhanced cascading failure model integrating data mining technique," *Protection and Control of Modern Power Systems*, vol. 2, no. 2, pp. 19–28, 2017.

[9] Z. Chen, J. Wu, Y. Xia et al., "Robustness of interdependent power grids and communication networks: a complex network perspective," *IEEE Transactions on Circuits and Systems II*, vol. 65, no. 1, pp. 115–119, 2018.

[10] X. Ji, B. Wang, D. Liu et al., "Improving interdependent networks robustness by adding connectivity links," *Physica A: Statistical Mechanics and its Applications*, vol. 444, pp. 9–19, 2016.

[11] O. Yagan, D. Qian, J. Zhang et al., "Optimal allocation of interconnecting links in cyber-physical systems: interdependence cascading failures, and robustness," *IEEE Transactions on Parallel and Distribution Systems*, vol. 23, no. 9, pp. 1708–1720, 2012.

[12] J. Wang, C. Jiang, and J. Qian, "Robustness of interdependent networks with different link patterns against cascading failures," *Physica A: Statistical Mechanics and its Applications*, vol. 393, pp. 535–541, 2014.

[13] K. Schneider, C.-C. Liu, and J.-P. Paul, "Assessment of interactions between power and telecommunications infrastructures," *IEEE Transactions on Power Systems*, vol. 21, no. 3, pp. 1123–1130, 2006.

[14] Q. Wang, M. Pipattanasomporn, M. Kuzlu, Y. Tang, Y. Li, and S. Rahman, "Framework for vulnerability assessment of communication systems for electric power grids," *IET Generation, Transmission & Distribution*, vol. 10, no. 2, pp. 477–486, 2016.

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

[16] P. Huang, Y. Wang, and G. Yan, "Vulnerability analysis of electrical cyber physical systems using a simulation platform," in *Proceedings of the IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, pp. 489–494, Beijing, China, October 2017.

[17] Y. Deng, H. Lin, S. Shukla et al., "Co-simulating power systems and communication network for accurate modeling and simulation of PMU based wide area and measurement systems using a global event scheduling technique," in *Proceedings of the Workshop on MSCPES*, p. 1, Berkeley, CA, USA, May 2013.

[18] S. Tan, W. Song, D. Huang, Q. Dong, and L. Tong, "Distributed software emulator for cyber-physical analysis in smart grid," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 506–517, 2017.

[19] M. Rana, "Architecture of the internet of energy network: An application to smart grid communications," *IEEE Access*, vol. 5, pp. 4704–4710, 2017.

[20] S. E. Collier, "The emerging enernet: convergence of the smart grid with the internet of things," *IEEE Industry Applications Magazine*, vol. 23, no. 2, pp. 12–18, 2017.

[21] D. Dzung, M. Naedele, T. P. von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, 2005.

[22] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, 2013.

[23] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2017.

[24] G. N. Ericsson, "Cyber security and power system communication-essential parts of a smart gird infrastructure," *IEEE Transactions on Power Delivery*, vol. 25, no. 3, pp. 1501–1507, 2010.

[25] R. K. Pandey and M. Misra, *Cyber Security Threats-Smart Grid Infrastructure*, NPSC, Bhubaneswar, India, 2016.

[26] D. Wang and H. Qin, "Design and application of antivirus system in Qinghai electric power dispatching data network," *Qinghai Electric Power*, vol. 31, no. 3, pp. 61–63, 2010.

[27] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, 2013.

[28] X. Wei, J. Zhao, T. Huang, and E. Bompard, "A novel cascading faults graph based transmission network vulnerability assessment method," *IEEE Transactions on Power Systems*, vol. 33, no. 3, pp. 2995–3000, 2018.

[29] X. Wei, S. Gao, T. Huang et al., "Identification of two vulnerability features: a new framework for electrical networks based redistribution mechanism of complex networks," *Complexity*, vol. 2019, Article ID 3531209, 14 pages, 2019.

[30] B. Qu and H. Wang, "SIS epidemic with heterogeneous infection rates," *IEEE Transaction on Network Science and Engineering*, vol. 4, no. 3, pp. 177–186, 2018.

[31] I. Tomovski and L. Kocarev, "Simple algorithm for virus spreading control on complex networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 59, no. 4, pp. 763–771, 2012.

[32] Y. Tang, X. Han, Y. Wu et al., "Electric power system vulnerability assessment considering the influence of communication system," in *Proceedings of the*, vol. 35, pp. 6066–6074, 2015.

[33] Z. Lu, Z. Meng, and S. Zhou, "Cascading failure analysis of bulk power system using small-world network model," in *Proceedings of the International Conference on Probabilistic Methods Applied to Power Systems*, pp. 635–640, Ames, IA, USA, 2004.

[34] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the Italian electric power grid," *Physica A: Statistical Mechanics and its Applications*, vol. 338, no. 1-2, pp. 92–97, 2004.

[35] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the European power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 7, pp. 2465–2475, 2007.

[36] G. Li, W. Ju, X. Duan et al., "Transmission characteristics analysis of the electric power dispatching data network," *Proceedings of the CSEE*, vol. 32, no. 22, pp. 141–148, 2010.

[37] J. Hu, Z. Li, and X. Duan, "Structural feature analysis of the electric power dispatching data network," *Proceedings of the CSEE*, vol. 29, no. 4, pp. 53–59, 2009.

[38] M. Romero-L and L. Gallego, "Analysis of voltage sags propagation in distribution grids using a SI epidemic model," in *Proceedings of the 3rd IEEE Workshop on Power Electronics and Power Quality Applications, PEPQA 2017*, Bogota, Colombia, June 2017.

[39] B. Jia, S. Liu, T. Zhou, and Z. Xu, "Opportunistic transmission mechanism based on si in mobile crowd sensing networks," in *Proceedings of the 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 211–215, Prague, Czech Republic, July 2017.

[40] P. Crépey, F. P. Alvarez, and M. Barthélemy, "Epidemic variability in complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 73, no. 4, Article ID 046131, 2006.

[41] D. Xu and X. Xu, "Modeling and control of dynamic network SIR based on community structure," in *Proceedings of the 26th Chinese Control and Decision Conference, CCDC 2014*, pp. 4648–4653, China, June 2014.

[42] Z. Sun, B. Wang, J. Sheng, Y. Hu, Y. Wang, and J. Shao, "Identifying influential nodes in complex networks based on weighted formal concept analysis," *IEEE Access*, vol. 5, pp. 3777–3789, 2017.

[43] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 63, no. 6, Article ID 066117, 2001.

[44] Y. Moreno, R. Pastor-Satorras, and A. Vespignani, "Epidemic outbreaks in complex heterogeneous networks," *The European Physical Journal B*, vol. 26, no. 4, pp. 521–529, 2002.

[45] Y. Tang, X. Han, and Y. Wu, "Electric power system vulnerability assessment considering the influence of communication system," *Proceedings of the CSEE*, vol. 35, no. 23, pp. 6066–6074, 2015.

[46] A. Delavari and I. Kamwa, "Improved optimal decentralized load modulation for power system primary frequency regulation," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 1013–1025, 2018.

[47] Y. Guo, D. Zhang, J. Wan, and D. Yu, "Influence of direct air-cooled units on primary frequency regulation in power systems," *IET Generation, Transmission & Distribution*, vol. 11, no. 17, pp. 4365–4372, 2017.

[48] X. Yu and C. Singh, "A practical approach for integrated power system vulnerability analysis with protection failures," *IEEE Transactions on Power Systems*, vol. 19, no. 4, pp. 1811–1820, 2004.

[49] Y. Cao, Y. Zhang, and Z. Bao, "Analysis of cascading failures under interactions between power grid and communication network," *Dianli Zidonghua Shebei/Electric Power Automation Equipment*, vol. 33, no. 1, pp. 7–11, 2013.

[50] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.