Accepted Manuscript

Integrated Fault Propagation Model Based Vulnerability Assessment of the Electrical Cyber-Physical System under Cyber Attacks

Tianlei Zang , Shibin Gao , Baoxu Liu , Tao Huang , Tao Wang , Xiaoguang Wei

PII: S0951-8320(18)31290-0
DOI: https://doi.org/10.1016/j.ress.2019.04.024
Reference: RESS 6471

To appear in: *Reliability Engineering and System Safety*

Highlights

- We model the cascading failures of electrical CPS.
- We construct the two graphs to analyze the vulnerability of electrical CPS.
- We employ two graphs to construct the vulnerability indices.

Integrated Fault Propagation Model Based Vulnerability Assessment of the Electrical Cyber-Physical System under Cyber Attacks

Tianlei Zang[1,2], Shibin Gao[1], Baoxu Liu[3], Tao Huang[4,5], Tao Wang[5], Xiaoguang Wei[1]

1. School of Electrical Engineering, Southwest Jiaotong University, Chengdu, China
2. Department of Electrical Engineering, Tsinghua University, Beijing, China
3. Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences, Beijing, China
4. Department of Energy, Politecnico di Torino, Torino, Italy
5. School of Electrical Engineering and Electronic Information, Xihua University, Chengdu, China

Corresponding author: Tao Huang(tao.huang@polito.it) and Xiaoguang Wei(wei_xiaoguang@126.com)

Abstract：*This paper aims to identify the vulnerability of electrical cyber-physical systems (CPSs) through fault propagation under cyber attacks. First, we propose a fault propagation model mainly considering the impact of interruptions on some nodes of the cyber network on the electrical physical systems. Secondly, two graphs, i.e. propagation graph and attack graph are proposed to reveal the physical fault propagation mechanisms and analyze the attack intensity of combinations of different communication nodes, respectively. Thirdly, a set of traditional vulnerable indices based on the propagation and attack graphs are employed to identify both the critical physical branches and communication nodes in the CPS. Finally, comparative analyses with and without considering the CPS on both IEEE 118- and 300- bus systems show that the fault propagation among are more sophisticated and the wrong decisions that the control center makes causes the higher vulnerability of the electrical network due to the interruption of the transmission information in the cyber system under cyber attacks.*

Keywords：vulnerability, electrical cyber physical systems, fault propagation, cyber attacks

1. Introduction

With the intelligent development of the electrical network, there are increasingly closer coupling between cyber systems and electrical systems [1][2], which is gradually developing into an electrical cyber-physical system (CPS) [3][4].

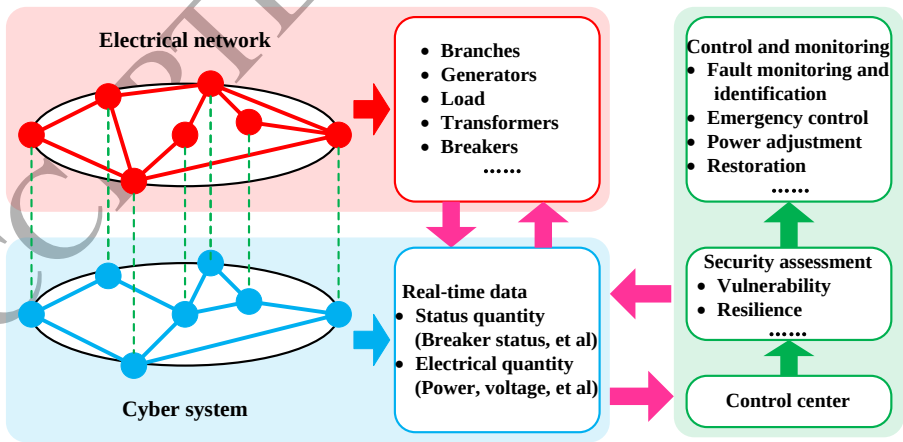


Figure 1. Framework of electrical CPS

The electrical CPS is an interdependent and integrated system of power system (e.g. physical system) and cyber system. The cyber system is a very important control and monitoring system to ensure the power system (e.g. physical) security, as shown in Fig. 1. It usually includes measurement units, control units, protection units, communication infrastructure, decision making software, e.g. EMS, SCADA, etc. The

real-time data of the electrical network including equipment status and measurements are sent by the cyber system to the control center [5]. Meanwhile the control center analyzes the received data and makes decisions based on it. Then corresponding control commands are sent back via the cyber system to relevant equipment when it is needed. In addition, many distributed control systems (DCSs) are also functioning as local decision units under the supervision of the control centers to perform quick and local controls; therefore the cyber system performs an important intermediate function between electrical network and control center. Once the cyber system fails which may be out of touch between control center and electrical network, the electrical network could be in an unsecure operational state. Therefore, the secure operation of the electrical physical system highly depends on the reliable and accurate real-time information transmitted by the cyber system as well as its DCSs. Meanwhile, with the advancement of smart grids, and the Internet of Things, the internet will be accessed by the grid at all levels (from the control center to equipment inside a household) to realize the real-time interaction between users and systems [6]. Although the electrical network can greatly benefit from effective monitoring and control of the cyber systems, cyber security must be prioritized [7]. For instance, cyber-attacks including unauthorized login, malicious code on the cyber system can cause the delay of data transmission and even data tampering/ lost [8][9]. In these cases, the control center cannot make reasonable decisions due to the lack of data or data delay. Particularly, when failure occurs in the power grid, the control center must quickly provide effective control via the cyber system to prevent cascading failures. However, due to the integration with the physical system, i.e. the electrical CPS, the attack at the cyber system can influence the grid operation and may bring even more serious consequences[10][11].

To analyze the impact of the cyber system on the electrical network, from the perspective of vulnerability assessment, reference [14] introduces a framework for the vulnerability assessment of the communication network considering the probability and consequence of interruption of communication service for the electrical network. The cyber-physical contingency analysis tool is employed to assess cyber-physical vulnerability by considering the cyber network configurations and power system topology in [15]. Meanwhile, [16] considers the incomplete information to model cyber-physical vulnerability of the smart grid. The above studies demonstrated that some vulnerable points in communication networks can create great damages for electrical networks; therefore the fault mechanism of the electrical network becomes more complex and uncertain. Especially, some attacked communication nodes can lead to adverse blackout in the electrical system.

To reveal cascading propagation features under the interference of communication failures, different connectivity modes (i.e., coupled modes) between communication networks and electrical networks from a topological perspective are investigated. Reference [17] reveals that the double-network link allocation strategy is superior to single-network link allocation strategy. Meanwhile, from the perspective of protective effect and computing efficiency, some studies demonstrate that we can improve the robustness of interdependent networks by link addition strategy [18][19].

Although the above mentioned methods reveal the relationships between cascading failures and different types of links between electrical networks and communication networks, it is not comprehensively enough to reveal the fault propagation mechanism only from a pure topological perspective, which ignores the operational features of electrical network during the fault propagation; therefore some studies focus on integrating the operational features of electrical networks under interdependent fault propagation. Especially, the impacts of different topological properties of communication networks on operational features of electrical networks are analyzed [20][21]. Reference [5] models the interactive cascading failures by considering different topological structures of the communication system, which concludes that the electrical network coupled with a scale-free communication structure [12] has a lower probability of cascading failures than that with a small-world structure [13].

The blackout of the Ukrainian grid in 2015 is a typical event due to a cyber-attack [22]. The attackers successfully sent a fake command to the Ukrainian grid, leading to the system-wide power outage. In the

event, one of the main ways of the attack is to disable the information exchanges channel between the communication nodes and control center in the cyber-system (Fig. 2) by uploading malicious code to the servers or workstations of the communication nodes [23], which results in the control center cannot monitor and control the operational state of the substations coupled with attacked communication nodes.

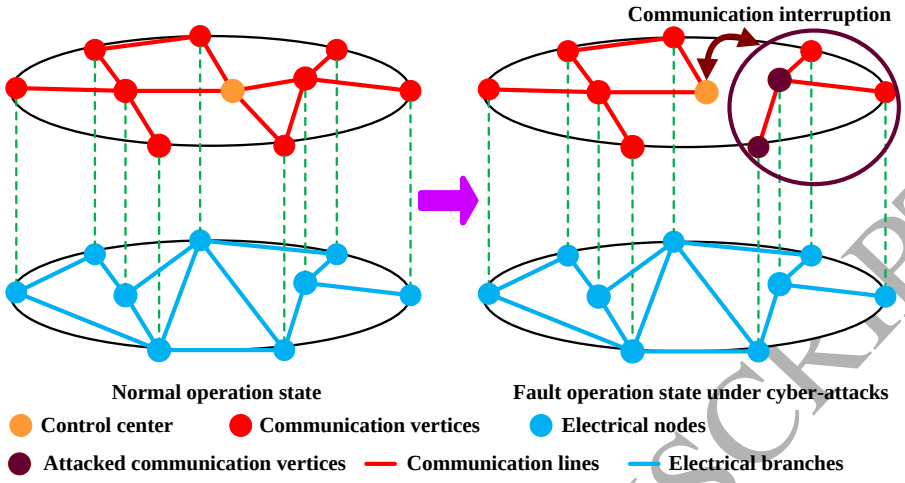


Figure 2. Diagram of cyber-attacks

Inspired by the blackout of the Ukrainian grid, we would like to investigate the vulnerability of the CPS under cyber-attacks. Unlike other studies for the fault propagation paths which only consider the physical attacks by removing branches in the electrical system, our investigation evaluates the impact of the cyber system failure on the fault propagation paths in the electrical systems by directly considering the interdependence between the electrical and communication networks in the fault propagation model. It is noted that the physical attacks are to directly remove the targeted branches from the electrical networks without considering the impacts of communication networks. Based on the newly proposed fault propagation model, we constructed the attack graph and vulnerable indices as means to compared the differences. Thus, we designed the following steps: 1) We propose an interdependent fault propagation model to replicate the interactions between the electrical physical network and the cyber system inside the CPS. 2) Propagation graphs based on the fault propagation model are proposed to record the mechanism of the propagation. Meanwhile, we construct attack graphs to analyze the gravity of consequences of attacks on the physical system with different combinations of initially attacked communication nodes. 3) The propagation graphs and attack graphs are then used to construct vulnerability indices to assess the electrical CPS vulnerability.

The contributions of this paper can be summarized as:

First, to reveal the fault propagation mechanism under cyber attacks, we model the cascading failures of electrical CPS according to the experience of the Ukraine cyber attack.

Secondly, to analyze the vulnerability of the electrical CPS, two graphs (e.g. propagation graph and attack graph) are constructed based on the cascading failure model.

Thirdly, we employ two graphs to construct the vulnerability indices to identify the critical transmission branches and communication nodes of the electrical CPS.

The remainder of this paper is organized as follows. Section 2 describes the informational interactions inside the electrical CPS and models the cascading failures of the electrical CPS under cyber attacks. In Section 3, the generation methods of two graphs are proposed in detail and then vulnerability indices are constructed to assess the CPS vulnerability. The IEEE 118- and 300-bus systems are employed to verify the validity of the proposed methods in Sections 4. Finally, conclusions are drawn in Section 5.

2. Informational Interactions inside the Electrical CPS

2.1 Data exchange in the electrical CPS

In a CPS, a communication node can only exchange information packets with its neighbor nodes [5]; therefore information transmission depends on the topological structure of the CPS. When the source node produces information packets, if the control center is its neighbor node, the information packets are directly sent to the control center and the information transmission ends. Otherwise, the information packets travel through the shortest path from the source node to the control center via a set of nodes.

We denote the distance between two arbitrary nodes *i* and *j* through a path with less than k nodes as d_{ij}^{k}, $i, j \in 1,2,\ldots,N_R$ $k \in \mathbb{Z}_0^+$. if $\exists M>0, k<M, k \in \mathbb{Z}_0^+$ such that $d_{ac} = d_{ar}^{k} + d_{rc}^{k} < \infty$, then we define ρ_{ac} =1, otherwise, ρ_{ac} =0 as in (1), where V_a (a=1,2,…,N_R , N_R is the number of communication nodes) and V_c is the communication node of the control center.

$$\rho_{ac} = \begin{cases} 1 & \exists d_{ac} \\ 0 & \neg \exists d_{ac} \end{cases} \tag{1}$$

Furthermore, because the needed time for information exchange between two nodes is typically in a range of milliseconds while the reestablishment of power balance in the power system is in the scale of minutes, we ignore the time of information exchange in this paper. In addition, the "first-in-first-out" rule is assumed for a communication node in processing information packets, i.e., the communication node dispatches/transmits the received data packages in accordance to the sequence of receipt, regardless of the time labels embedded in the packages.

Moreover, in the electrical CPS, we consider a one-to-one interdependent network, i.e., each bus in the electrical physical network has a corresponding communication node in the CPS. It should be noted that the topological structures of the two sub-systems are not necessarily identical. In general, the communication network and the physical network has no one-to-one match from the structural point of view. Most of them are even one-to-many configuration. The one-to-many match can have a lower security level compared to the one-to-one match because it can cause many electrical nodes not be able to communicate with the coupled communication node once the communication node fails. Thus the one-to-many configuration is commonly used in the low voltage level which has lower impact. But for important equipment or high voltage level, the one-to-one configuration is more viable. In our study, we assumed a high voltage level transmission network, thus the one-to-one assumption is surely valid. In addition, we make further simplifications that for each transmission branch, we assume the communication node is coupled with one bus of the branch.

It is noted that if the one-to-many configuration is assumed, as mentioned above, the communication node failure will trip multiple branches rather than the ones connected to the same bus, but obviously, it will not change the effectiveness of the proposed methods, as a high voltage bus failure will also trip multiple branches connected to it and also makes some down-stream buses out of power supply as well.

2.2 Overload mechanism in the transmission networks

In this paper, the fault propagation is studied from the perspective of the overload mechanism [24][25][26], i.e., in a transmission network, when one or more branches fail, the load of the entire network will redistribute, which may cause other branches overloaded and tripped. In addition, it is noted that as media connecting equipment in the power system, the electrical transmission network has very fast dynamics/transients when compared with power electronics or rotating devices. In other words, the transmission grid per se does not have such dynamic issues. Thus, the dynamic/transient stability features of generators or loads are not considered and only protections related to the transmission branch are modeled.

Load redistribution: The PQ decomposition method [27] is employed to calculate the load redistribution of the entire network (2)-(3), where P_i and Q_i denote the net injection of active and reactive power of the bus

i. U_i and U_j represent the voltage amplitude of the buses i and j, respectively. $G_{ik}+jB_{ik}$ denotes the admittance between buses i and k. θ_{ik} denotes the difference of voltage angles between buses i and k. ΔP_i and ΔQ_i are the mismatches of the active and reactive power between the net power injection and calculated terms via admittances and voltages of the bus i.

$$\Delta P_i = P_i - U_i \sum_{k=1}^{n} U_k (G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik}) \tag{2}$$

$$\Delta Q_i = Q_i - U_i \sum_{k=1}^{n} U_k (G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}) \tag{3}$$

Control strategy: When branches overloaded due to an initial fault, to effectively avoid cascading failures, we re-dispatch the generators and shed load, if necessary, as the control strategy to relieve the overload. Thus a modified AC OPF [28] is used to minimize the load shedding δ in the electrical system (4).

$$\min\ \delta = \sum_{i=1}^{N_B} \delta_i \tag{4}$$

s.t.

$$P_i - \delta_i = U_i \sum_{k=1}^{n} U_k (G_{ik}\cos\theta_{ik} + B_{ik}\sin\theta_{ik})\ (i=1,2,\ldots,N_B) \tag{5}$$

$$Q_i = U_i \sum_{k=1}^{n} U_k (G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik})\ (i=1,2,\ldots,N_B) \tag{6}$$

$$P_{j\min}^{G} \le P_j^{G} \le P_{j\max}^{G}\ (j=1,2,\ldots,N_B) \tag{7}$$

$$Q_{j\min}^{G} \le Q_j^{G} \le Q_{j\max}^{G}\ (j=1,2,\ldots,N_B) \tag{8}$$

$$0 \le P_l^{L} \le P_{l\max}^{L}\ (l=1,2,\ldots,N_L) \tag{9}$$

$$U_{i\min} \le U_i \le U_{i\max}\ (i=1,2,\ldots,N_B) \tag{10}$$

$$0 \le P_m^{\mu} \le P_{m0}^{\mu}\ (m=1,2,\ldots,N_B) \tag{11}$$

Where N_B, N_L are represented the number of bus nodes and branches, respectively. δ_i represents the load shedding of the bus i. $P_{j\min}^{G}$ and $P_{j\max}^{G}$ are represented the upper and lower limits of the active power of the generator j. $Q_{j\min}^{G}$ and $Q_{j\max}^{G}$ are the upper and lower limits of the active power of the reactive power of the generator j. $P_{l\max}^{L}$ are represented the limit power of the branch L. $U_{i\min}$ and $U_{i\max}$ are represented the upper and lower limits of the voltage of the bus i. P_{m0}^{μ} are represented the load of the node m in normal operation. It is noted that although the AC OPF is used to adjust the overload as generally employed in existing studies, our fault propagation model collectively considers the impact of the information losses due to a cyber attack in the formation and analysis of the fault propagation path in the electrical system.

2.3 Fault propagation model

Fault propagation model under physical attacks: In the traditional fault propagation model, the model only considers the physical behaviors of the electrical networks and the physical attacks on the equipment is simply modeled by removing it from the system. From the perspective of the overload mechanism, when one or more branches are removed (i.e., physical attacks), the power distribution in the electrical network will change and may lead to other branches overloaded and tripped; therefore the simplified fault propagation model under physical attacks can be described as follows:

Algorithm 1: Fault propagation model under physical attacks
Input: Electrical network information.
Output: Cascading chain $\vec{L}=(L,R)$, where cascading events $L=\{L_x \mid x=1,2,\ldots,N_x\}$ and fault adjacent relationship $R=\{R_{(x-1)x} \mid R_{(x-1)x}=L_{x-1}\rightarrow L_x, x=1,2,\ldots,N_x-1\}$. L_x represents the set of overloaded

branches in the xth contingency. N_x represents the number of sets.

Choose the initial attacked branches in the electrical network; $x=1$

Add the initial attacked branches to set L_1.

WHILE

$x=x+1$;

Calculate the power flow of the electrical network using equation (3) and (4).

IF the overload branches exist, record the overloaded branches $L_x=\{L_{O_x}|O_x=1,2,\ldots,N_o^x\}$ and fault adjacent relationship $R_{(x-1)x}=L_{x-1}\rightarrow L_x$, where N_{O_x} is the number of overloaded branches; **ELSE**, **BREAK**.

END IF

Employ equations (4)-(8) and (11) to adjust the power of generators and loads.

END WHILE

Fault propagation model under cyber attacks: When a branch in the transmission network is overloaded, the coupled communication node can quickly send the fault information packets to the control center via the well functioning cyber network. After receiving the information, the control center can make corresponding control decision to relieve the overload by adjusting generators and loads if needed. The interaction process between the transmission network and the cyber system is shown in Fig. 3.

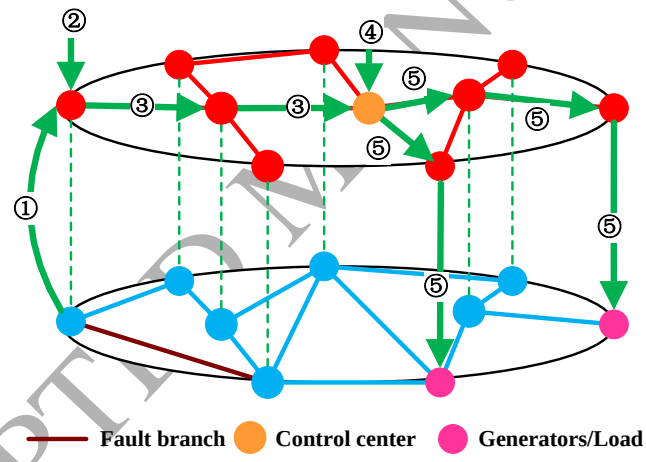


Figure 3. Informational interactions in the electrical CPS. ①: information collection ②: information packets production ③: information packets transmission ④: control strategy ⑤: command sending.

On the other hand, according to the experience of the Ukraine cyber attack, if a communication node in the CPS is attacked, it will lose its function, i.e. no information packets can go through it and the command from the control center cannot reach the corresponding equipment as well (Fig. 4.). Further, the associated physical equipment will be tripped. Of course, there are countermeasures to obtain such information if the number of lost packets is comparatively small, such as using state estimation of the EMS, etc. Yet, with coordinated attacks or a comparatively large scale attack, the currently in place countermeasure will be rendered ineffective.

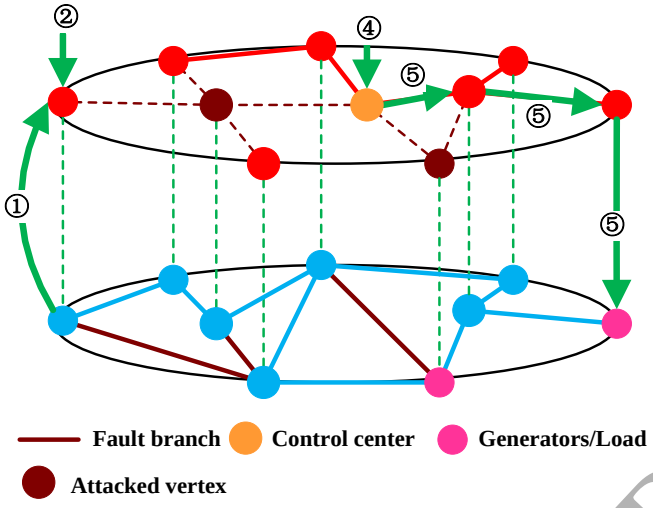


Figure 4. Informational interactions in the electrical CPS under communication node attack.

As the control center will loss the information on the attacked communication nodes with the coupled electrical nodes, as well as those who cannot establish a communication route with it, thus the control center will not consider them into their decision.

Fig. 5 shows the interactions of the physical system and the cyber system.

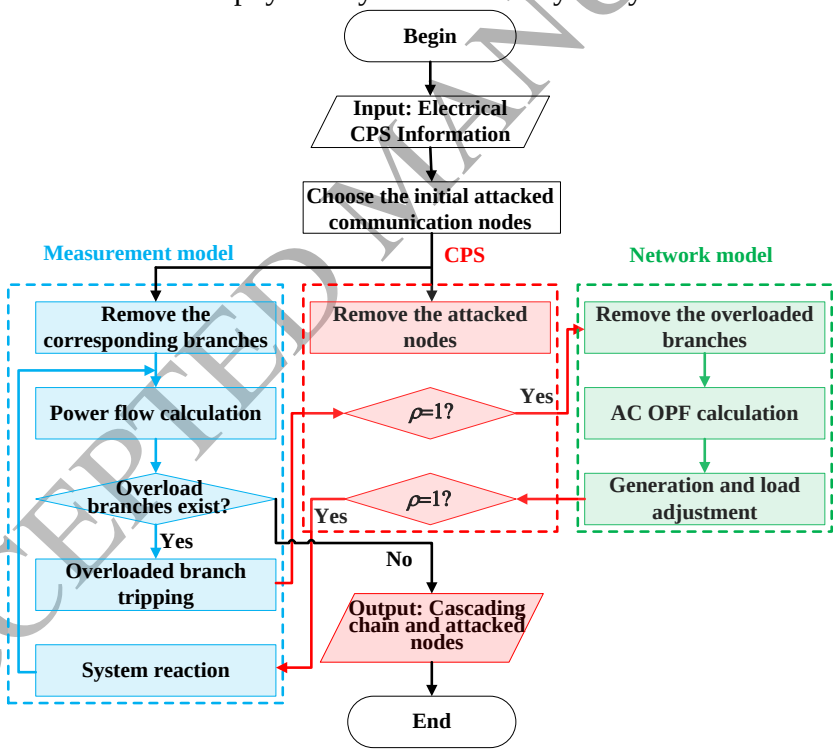


Figure 5 Fault propagation process

It should be noted that in this paper, the "measurements" will also be generated through a simulation with AC power flow; however, to avoid ambiguity, we still call them measurements.

Based on the above analysis, the fault propagation can be simulated as follows:

Algorithm 2: Fault propagation model under cyber attacks
Input: Electrical CPS information.

Output: Cascading chain $\vec{L}=(L,R)$ and combination of initial attacked communication nodes

Choose the initial attacked communication nodes in the CPS.

Remove the attacked nodes from the CPS while remove the corresponding branches from the measurement model.

Add the initial attacked branches to set L_1.

WHILE

$x=x+1$;

Power flow calculation: Calculate the power flow of the measurement model using equation (2) and (3).

Overloaded branch tripping: **IF** the overload branches exist, record the overloaded branches $L_x=\{L_{O_x}|O_x=1,2,\ldots,N_o^x\}$ and fault adjacent relationship $R=\{R_{(x-1)x}|R_{(x-1)x}=L_{x-1}\rightarrow L_x, x=1,2,\ldots,N_x-1\}$, where N_{O_x} is the number of overloaded branches; **ELSE**, **BREAK**.

END IF

FOR O_x =1: N_o^x

Branches tripping exchange: **IF** $\exists d_{oc}$ between the V_c and V_o coupled with the L_{O_x}, e.g., ρ_{oc}=1, remove L_{O_x} from the network model.

END IF

END FOR

AC OPF Calculation: Employ AC OPF (i.e., equations (4)-(11)) to adjust the power of generators and loads based on the network model.

Generation and load adjustment: The power adjustments of the generators and loads are $\{\Delta P_j^G \mid j=1,2,\ldots,N_G\}$ and $\{\Delta P_m^\mu \mid m=1,2,\ldots,N_\mu\}$, respectively.

FOR j=1: N_G (m=1: N_μ)

System reaction: **IF** $\exists d_{jc}$ ($\exists d_{mc}$) between V_c and V_j (V_m) coupled with the generator G_j (load μ_m), e.g., ρ_{jc}=1 ($\rho_{\mu c}$=1), adjust the power $P_j^G=P_j^G+\Delta P_j^G$ ($P_m^\mu=P_m^\mu+\Delta P_m^\mu$) of the generator G_j (load μ_m) in the measurement model.

END IF

END FOR

END WHILE

3. Vulnerability Analysis in the CPS

In order to assess the vulnerability of the CPS, we propose two graphs to first analyze the cyber and electrical systems, and then using two vulnerability indices to holistically analyze the vulnerability of the CPS.

3.1 Propagation graph and vulnerability index in the transmission network

Propagation graph (PG) of the transmission network: Based on the algorithm 1 or 2 of the fault propagation model, we can obtain a cascading chain $\vec{L}=(L,R)$, where cascading events is defined as $L=\{L_{O_x}|L_{O_x}\in L_x, x=1,2,\ldots,N_x\}$ and the fault adjacent relationship is determined by $R=\{R_{(x-1)x}|R_{(x-1)x}=L_{x-1}\rightarrow L_x, x=1,2,\ldots,N_x-1\}$. It should be noted that the fault in this paper refers to the branch overload. To measure the incremental severity of the failures in the transmission network from step x to x+1, we design equation (12) as the weight $W_{(x-1)x}$ of $R_{(x-1)x}$ between L_{x-1} and L_x.

$$W_{(x-1)x} = \frac{N_o^x}{N_o^{x-1}} \tag{12}$$

where N_o^x is the number of overloaded branches in the step *x*. Obviously, if the number of overloaded branches in the step *x*-1 is small but they can cause more branches tripping in the step *x*, the value of $W_{(x-1)x}$ would be larger, which indicates a higher gravity of consequence to the intactness of the transmission network in the step *x*.

Furthermore, to reveal the adjacent fault relationship among individual branches, a cascading chain can be divided into $\prod_{x=1}^{Nx} N_o^x$ sub-chains, i.e., $\vec{L}_q = (L_q, R_q)$, where $L_q = \{L_{O_x} | L_{O_x} \in L_x, x = 1,2,\ldots,N_x\}$ and $R_q = \{R_{O_{x-1}O_x} | R_{O_{x-1}O_x} = L_{O_{x-1}} \to L_{O_x}, L_{O_{x-1}} \in L_{x-1}, L_{O_x} \in L_x, x = 2,\ldots,N_x\}$. Further, we define the $W_{O_x O_{x+1}}$ of the $R_{O_{x-1}O_x}$ as $W_{(x-1)x}$. To obtain a more general result, we use the Monte Carlo Method to generate *M* cascading events and then capture $M \times \prod_{u=1}^{Nc} N_o^u$ sub-chains. For every sub-chain $\vec{L}_q = (L_q, R_q)$, we employ mapping function $\Gamma : \vec{L}_q \to g_q$ to convert the sub-chain $\vec{L}_q$ to a weighted and directed graph g_q, i.e., $g_q = \Gamma(\vec{L}_q)$. For the g_q, we define $g_q = \langle v_q, e_q \rangle$ as follows:

1) The set of overloaded branches L_q in the electrical system is converted to a set of vertices v_q, i.e., $V_q = \Gamma(L_q)$ in a graph. The set of vertices is denoted as $V_q = \{V_{O_x} | V_{O_x} = \Gamma(L_{O_x}), L_{O_x} \in L_x, x = 1,2,\ldots,N_x\}$.

2) The set of fault adjacent relationships R_q in the electrical system is converted to a set of directed and weighted edges e_q, i.e., $e_q = \Gamma(R_q)$ in the graph. The set of edges is denoted as $V_q = \{e_{O_{x-1}O_x} | e_{O_{x-1}O_x} = \Gamma(R_{O_{x-1}O_x}), x = 2,3,\ldots,N_x\}$, where the weight of $e_{O_{x-1}O_x}$ is defined by $W_{(x-1)x}$.

By the above-defined mapping operator, we can obtain $M \times \prod_{x=1}^{Nx} N_o^x$ weighted and directed sub-graphs. Then, we employ equation (13) to generate a propagation graph g.

$$g = \left\{ (v, e) | v = \bigcup_{q=1}^{M \times \prod_{x=1}^{Nx} N_o^x} v_q, e = \bigcup_{q=1}^{M \times \prod_{x=1}^{Nx} N_o^x} e_q \right\} \tag{13}$$

Suppose an edge $e \in v$ in the propagation graph g satisfies $e \in v_1$ in g_1, $e \in v_2$ in $g_2 \ldots$, $e \in v_t$ in g_t, where its weights are W_e^1, $W_e^2, \ldots$, W_e^t in $g_1, g_2 \ldots, g_t$, respectively. We define the weight W_e of e in g as

$$W_e = W_e^1 + W_e^2 + \ldots + W_e^t \tag{14}$$

In addition, because the propagation graph consists of several cascading chains; therefore the propagation graph is a statistical graph which can reveal the main fault propagation path of a network.

PG based vulnerability index (PGVI): In the propagation graph, we adopt node degree [29] as equation (15) to measure the vulnerability of vertex V_l (i.e., branch L_l), called PGVI.

$$D_l = \sum_{v=1}^{|V|} e_{lv} \tag{15}$$

where e_{lv} (v=1,2,…,N_L) represents the adjacent relationships between the vertex L_l and L_v. If L_v is the neighbor of L_l, then e_{lv}=1; otherwise e_{lv}=0. It is obvious that the higher degree of L_l, the more vulnerable the branch L_l is. This feature indicates that the branch L_l can be easily effected by a fault or/and can easily spread a fault.

3.2 Attack graph and vulnerability index in the cyber system

Attack graph (AG) of the cyber system: We construct an attack graph of the cyber system to investigate what combinations of communication node attacks can both easily trigger fault propagations in the transmission network and cause higher damages. In other words, the attack graph is constructed to reveal the attack capabilities under different combinations of communication nodes.

Suppose a combination of attacked communication nodes includes $V_R = \{V_r \mid r=1,2,\ldots,N_r\}$, where N_r is the number of attack nodes. We add an edge E_{rt} between two attacked nodes edges V_r and V_t, where $E_{rt} \in E_R = \{E_{rt} \mid V_r \in V_R, V_t \in V_R, r \neq t\}$ as shown in Fig. 6.

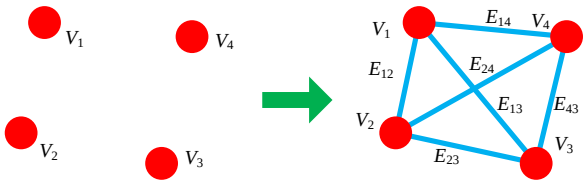


Figure 6 Generation diagram of graph

Thus, the combination can be viewed as the graph $G_R = \langle V_R, E_R \rangle$. The weight W_{rt} of the edge E_{rt} is defined as

$$W_{rt} = \frac{N_F}{N_r} \tag{16}$$

where N_F is the number of fault branches triggered by the attacked nodes, which signifies the gravity of the communication nodes attack. Manifestly, with the same number of attacked communication nodes, the larger the W_{rt} is, the more severe the attack is, that is, the greater weights of edges between two communication nodes demonstrate that when the two communications as a combination are simultaneously attacked, the electrical network can be destroyed more seriously with high probability. Suppose there are M combinations, i.e., $G_1, G_2, \ldots, G_M$, the attack graph G can be constructed as

$$G = \left\{ (V, E) \mid V = \bigcup_{R=1}^{M} V_R, E = \bigcup_{R=1}^{M} E_R \right\} \tag{17}$$

Similarly, the weights of edges in G are defined based on equation (14).

AG based vulnerability index (AGVI): In general, high degree indicates high vulnerability. Thus, in the attack graph, when an attacked combination contains a high degree communication node, the combination can easily trigger a cascading event and has a large impact on the electrical network. Therefore, we employ the degree of communication nodes based on the AG to measure the ability of the node V_r to trigger the cascading event, called AGVI.

$$D_r = \sum_{t=1}^{N_r} E_{rt} \tag{18}$$

where E_{rt} (v=1,2,…,N_r) represents the adjacent relationships between the vertex L_r and L_t. If L_t is the neighbor of L_r, then E_{rt}=1; otherwise E_{rt}=0.

3.3 CPS vulnerability indices from the perspective of information transmission

Center betweenness (CB): In the CPS, we employ the betweenness [30] as in (19) to measure the information transmission capability of the communication nodes. A high betweenness of the communication node V_a indicates a more important role in the process of information exchange.

$$b_a = \sum_{r \in V} \sum_{t \in V\,(r \neq t)} \frac{\sigma_{rt}(a)}{\sigma_{rt}} \tag{19}$$

where $\sigma_{rt}(a)$ represents the number of shortest paths via node V_a between node V_r and V_t. σ_{rt} represents the number of shortest paths between nodes V_r and V_t.

In our study, as the most important information exchange would be from the source nodes to the control center; therefore (20) can be used to calculate the information transmission capability between the communication nodes and the control center. Based on the topological structure of the cyber system, the betweenness, called CB, of the node V_a is

$$b_a = \sum_{r \in V} \frac{\sigma_{rc}(a)}{\sigma_{rc}} \tag{20}$$

where $\sigma_{rt}(a)$ is the number of shortest paths via node V_a between any arbitrary node V_r and control center V_c. It is noted that compared with the attack graphs based AGVI that employed to analyze the capacity of a node triggering a cascading event, the CB is based on the topological structure of the cyber system, and is used to analyze the importance of a communication node on the paths for information transmission.

Interactive betweenness (IB): As a vulnerable branch is highly important to the transmission network, the level of the robustness of the corresponding communication node must be strengthened so that it can reliably send the measurements and fault information of the branch to the control center. However, from the perspective of the electrical CPS, if the corresponding communication node of the vulnerable branch is attacked, leading to the loss of the vulnerable branch, the impact on the physical system can be also huge. Consequently, the corresponding communication node is rendered to be vulnerable in the electrical CPS. To quantify it, we propose the interactive betweenness as in (21) to assess the CPS vulnerability.

$$b'_a = D_l \sum_{r \in V} \frac{\sigma_{rc}(a)}{\sigma_{rc}} = \sum_{v=1}^{|V|} e_{lv} \sum_{r \in V} \frac{\sigma_{rc}(a)}{\sigma_{rc}} \tag{21}$$

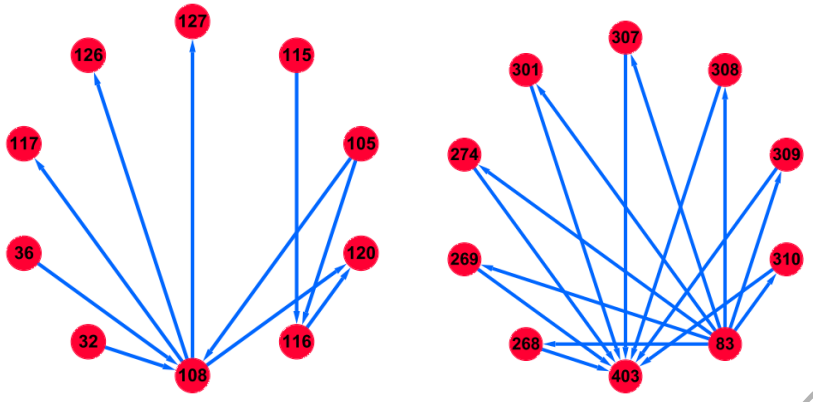
where D_l is the degree of the communication node V_r coupled with the branch L_l. b'_a considers not only the importance of a communication node, but also the vulnerability of the corresponding branch of the node; therefore b'_a can comprehensively reveal the vulnerability of the communication node.

4. Case Study

We employ IEEE 118- and 300- bus systems to illustrate the proposed method. 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. We simulate M=1000 cascading events to construct the propagation graphs and attack graphs of the IEEE 118- and 300- bus systems.

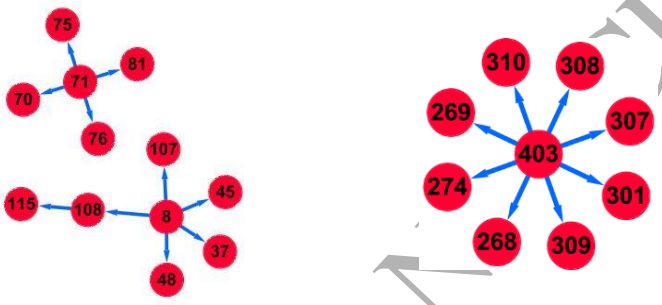
4.1 Electrical network vulnerability analysis

We employ the 1000 cascading events to generate the propagation graphs of the IEEE 118 and 300- bus systems according to equation (13). In the propagation graphs, because there exists many low weighted edges among branches, it indicates it is difficult to spread a fault among branches. Therefore, to focus on the main propagation paths, we extract the high weighted edges from the propagation graph, as shown in Fig. 7. Meanwhile, to compare with cyber attacks, we directly attack the electrical network (i.e., physical attacks) without considering the interactions inside the CPS. Under the physical attacks, the high vulnerable propagation graph is shown in Fig. 8. In the IEEE 118-bus system, under cyber attacks, (36, 32, 105)-108-(126,127,120) and (115, 105)-116-120 are high vulnerable propagation paths. Compared with the cyber attacks, 54-19, 71-(75, 70, 81, 76), 8-(107, 45, 37, 48) and 8-108-115 the high vulnerable propagation graph under physical attacks. Meanwhile, in the IEEE 300-bus system, 83-(268, 269, 274, 301, 307, 308, 309, 310)-403 is high vulnerable propagation path under cyber attacks while 403-(274, 269, 310, 308, 307, 301, 309, 268) are high vulnerable propagation path under physical attacks. By comparison, the high vulnerable propagation paths have significant differences between two types of attacks. Especially, in the 300-bus system, under cyber attacks, branch 403 can be easily affected by a fault but can spread a fault under physical attacks. It demonstrates the interactions between electrical network and cyber system have great impacts on the fault propagation, that is, propagation path will change due to the interactions; therefore in the electrical CPS, electrical network vulnerability depends on not only the electrical network itself but also the cyber system, which causes fault propagation mechanism becomes more complex due to the interdependent interactions.



(a) *(b)*

Figure 7 High vulnerable propagation graphs under cyber attacks. (a) IEEE 118-bus system (b) IEEE 300-bus system.



(a) *(b)*

Figure 8 High vulnerable propagation graphs under physical attacks. (a) IEEE 118-bus system (b) IEEE 300-bus system.

In addition, by contrasting Figs. 7 and 8, the connection of fault propagation among branches under cyber attacks is more close and complex than that under physical attacks. It indicates that the wrong decisions that the control centers make will further aggravate the deterioration of the electrical networks.

Furthermore, we employ the BGVI of the propagation graph based on equation (15) to rank the vulnerable branches. The top 10 vulnerable branches are shown in Tab. I. Branches 108, 54, 96, 116 and 8 in the 118-bus system and branches 403, 83, 44, 360 and 361 in the 300- bus system are most vulnerable branches under cyber attacks while branches 8, 54, 32, 3 and 108 in the 118-bus system and branches 50, 88, 407, 44 and 90 in the 300- bus system are most vulnerable branches under physical attacks. Table 1 shows that the vulnerable branches have obvious differences between two types of attacks. It indicates that the cyber systems have a crucial impact on the electrical networks; therefore the vulnerability of the electrical CPS must be assessed holistically.

In summary, under cyber attacks, due to the incomplete information of the electrical networks, some incomprehensive or wrong decisions will facilitate the fault propagation among branches; therefore the control center must improve the ability to obtain and identify the information under cyber attacks.

Table 1 Top 10 vulnerable branches Based on PGVI

Rank	118-bus system		300-bus system		Rank	118-bus system		300-bus system	
	PA	CA	PA	CA		PA	CA	PA	CA
1	8	108	320	403	6	104	104	50	48
2	54	54	403	83	7	37	3	88	268
3	32	96	55	44	8	96	107	407	117
4	3	116	273	360	9	107	36	44	365
5	108	8	41	361	10	116	51	90	191

(PA: Physical attacks; CA: Cyber attacks)

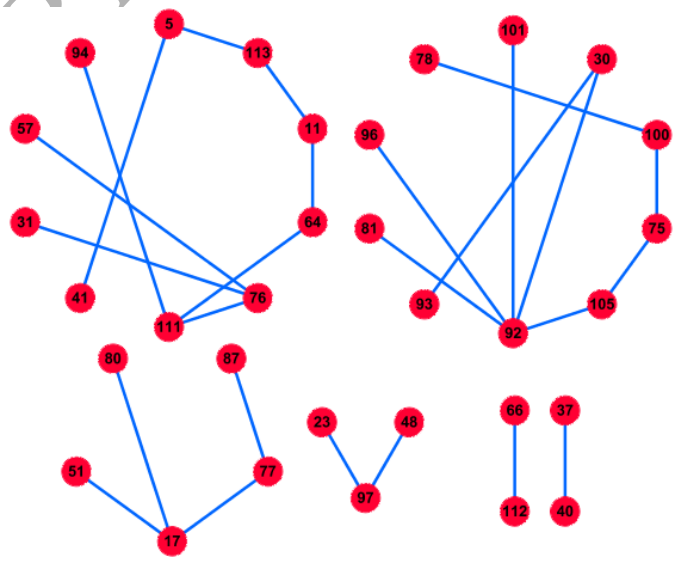
4.2 CPS vulnerability analysis

Similarly, we still choose the high vulnerable edges (i.e., the edges with great weights) to construct the high vulnerable attacked graph, shown in Fig. 9. Take the IEEE 118-bus system as an example, the high vulnerable attacked graph can be divided into five groups. In each group, if we choose the communication nodes which have the adjacent relationships among them as the attacked combinations, they can yield strong attacks which have the great damage for the electrical network. Among these groups, the fourth (56, 112) and fifth (37, 40) groups have small communication nodes; therefore if taking the two groups directly as the attacked combinations, the attackers may achieve their attack intentions at minimal cost. In addition, the AGVIs of attacked graphs are employed to rank the communication nodes shown in Tab. 2. In the IEEE 118-bus system, when nodes 92, 5, 101, 8 and 77 are attacked, they may easily trigger the cascading events and have high damage for the electrical network with high probability. To further verify the effectiveness of the proposed AGVIs, we attack the top critical nodes ranked by AGVI and compare the results, assessed by the number of tripped branches in the fault propagation process, with random attack, as shown in Fig. 10. As we see from Fig.10, compared with random attack, the number of tripped branches in each fault step after the removal of nodes identified by the AGVIs is more and the fault propagation steps in two IEEE bus systems are also longer; therefore it can infer that the electrical network can be destroyed seriously once the suggested communication nodes identified by the our method are attacked.

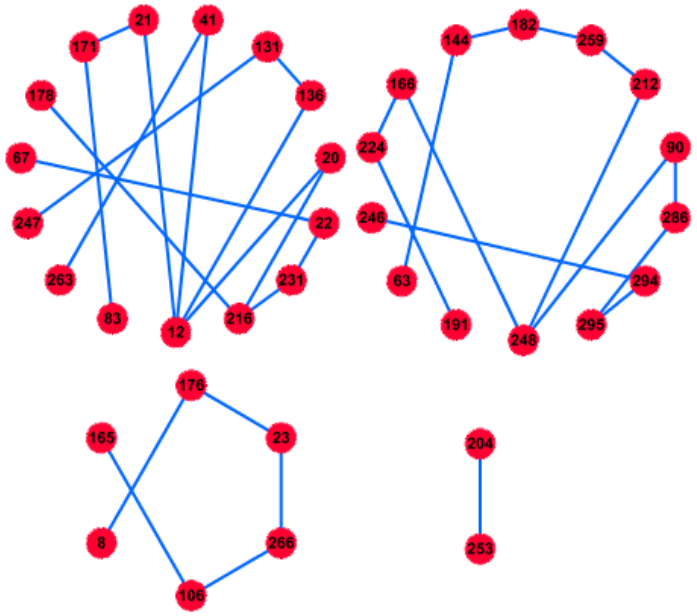
Table 2 Top 10 vulnerable branches Based on AGVI

Rank	118-bus system	300-bus system	Rank	118-bus system	300-bus system
1	92	248	6	111	216
2	5	100	7	64	259
3	101	249	8	17	23
4	8	2	9	93	162
5	77	224	10	37	177

By analyzing, in the cyber system, we must take some measures to improve the safety level of associated vulnerable nodes, such as, the nodes in an attacked combination with high risk are corresponding to different protection systems, firewalls, networking rules, etc., so that the difficulties of combined attacks can be increased.

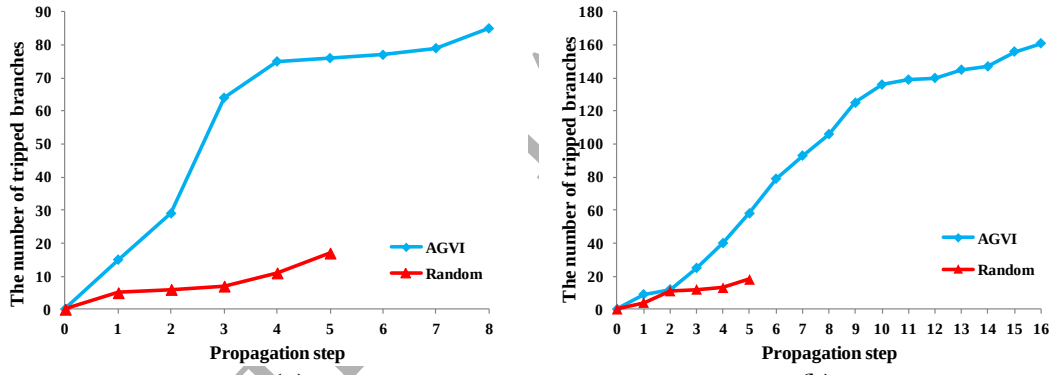


(a)



(b)

Figure 9. High vulnerable attacked graph. (a) IEEE 118-bus system (b) IEEE 300-bus system.



(a) *(b)*

Figure 10.Number of tripped branches under different attack mode. (a) IEEE 118-bus system (b) IEEE 300-bus system.

Meanwhile, we analyze the communication node vulnerability from the perspective of information transmission. The CB and IB are employed to rank the vulnerable nodes shown in Table3, respectively. By comparing CB and IB, there are obvious differences in the rankings. Take IEEE 118-bus system as an example, when pure topological structures of the cyber systems are only considered, the nodes 114, 116, 102, 115 in the electrical CPS are most vulnerable. By contrast, if the interactions between the cyber system and electrical network are considered, the nodes 37, 30, 114, 25 and 12 are most vulnerable. To further investigate the differences between CB and IB, we take the IEEE 118- bus system as an example and sequentially attacked the top nodes ranked by CB and IB, and compare the result, assessed by three indices: 1) The number of lost communication nodes, i.e., the communication nodes failing to exchange information with the control center in the communication network; 2) Network efficiency [11] of electrical network from the structural perspective; 3) Load shedding [25] of electrical system from the functional perspective. The results are shown in Fig. 11. In Fig. 11(a), the results identified by CB are obviously better than IB. It demonstrates that after attacking the suggested nodes ranked by CB, the more communication nodes fails to send the data

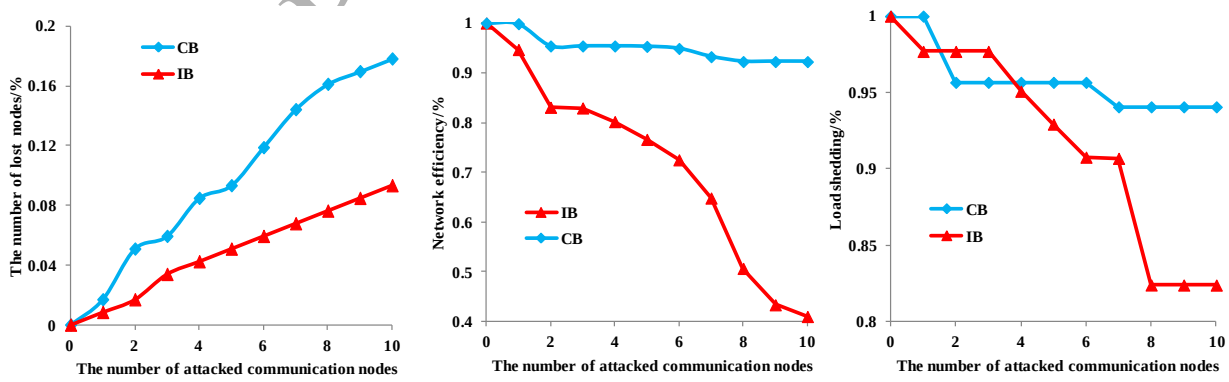
packages to control center compared with IB. It is not difficult to understand the reason that the CB is based on the pure topological structure of communication network.

However, in Fig, 11(b-c), the network efficiency and load shedding of electrical system after attacking the nodes identified by IB are generally less than that identified by CB. We can infer that the coupled branches with the attacked nodes identified by IB are more vulnerable than that identified by CB. Moreover, from the perspective of electrical CPS, the IB is better effectiveness to indentify the critical nodes than CB because the IB considers the interaction between electrical network and communication network; therefore the nodes identified by IB have greater impacts on the structure and function of electrical system.

In summary, due to the interactions between the cyber system and electrical network, fault propagation mechanism become more complex. From the perspective of electrical network, when cascading failures occur, the interactions can change the fault propagation path, leading to the increasing difficulty of control and prediction because the attacked communication nodes interrupt the information transmission between other communication nodes and the control center. From the perspective of the cyber system, to comprehensively assess the vulnerability of communication nodes, on the basis of considering the topological structures which can reflect the efficiency of information transmission, we also must consider the impacts of communication nodes on the structures and function of electrical networks once they are attacked.

Table 3 Top 10 Vulnerable Nodes Based on Different Indices

Rankings	118-bus system		300-bus system	
	CB	IB	CB	IB
1	114	37	298	198
2	116	30	280	217
3	102	114	285	213
4	115	25	299	95
5	98	12	297	216
6	110	34	273	186
7	112	65	295	122
8	111	69	296	168
9	63	70	294	182
10	48	23	293	18



(a) *(b)* *(c)*

Figure 11.Performance analysis after attacking communication nodes ranked by IB and CB for IEEE 118-bus system.(a)The number of lost communication nodes. (b)Network efficiency of electrical system. (c)Load shedding of electrical system.

In addition, by comprehensively analyzing Fig. 7-9, we can infer that if the physical network is only considered, generally, the smaller the scale of the network, the more sophisticated the relationships of fault propagation among branches and the more the high vulnerable propagation paths. On the contrary, due to the interactions of the electrical CPS, the larger scale of electrical network has more sophisticated propagation relationships; therefore we must deploy countermeasures to improve the security of cyber systems and mitigate or avoid cascading outages under cyber attacks.

5. Conclusions

The interactions between electrical network and CPS are receiving more and more attentions. In this paper, we focus on analyzing the fault propagation mechanisms of electrical CPS under cyber-attacks. We construct the cascading failure model by considering the impacts of transmission interruptions of the CPS under cyber-attacks on the electrical network. Meanwhile, to reveal the propagation path features of the electrical network under cyber-attacks, the propagation graphs are constructed based on the cascading failure model while the attacked graphs are constructed to analyze different combinations of initial attacked communication nodes for the damage level of electrical networks. Furthermore, from the perspective of interactions, we propose the indices based on propagation and attacked graphs to analyze the electrical network and CPS vulnerability, respectively. The numerical results on the IEEE 118- and 300- bus systems verify accuracy of our proposed method.

In this paper, we focus on constructing a fault propagation model under simultaneous cyber-attacks by considering the impact of different combinations of communication nodes on the electrical network. In the future, we can further investigate the fault propagation features under sequential or multi-stage cyber-attacks. Moreover, the cascading failures can be modeled from the perspective of time-scale to assess the vulnerability of electrical cyber physical systems. For instance, the time delay of information exchanges in the CPS can be considering during fault propagation.

In addition, in the next stage, we intend to introduce the clique/cluster to analyze which communication nodes are center nodes under different combinations, which may cause great damages for the CPS once they are attacked.

ACKNOWLEDGE

This work is supported by Key Program of National Natural Science Foundation of China (No. 51537006, 51877181 and 61703345) and Open Project of National Rail Transit Electrification and Automation Engineering Technique Research Center (No. NEEC-2017-B08).

References

[1] Huang K., Zhou C., Tian Y., et al. Assessing the physical impact of cyberattacks on Industrial cyber-physical Systems. IEEE Transaction on Industrial Electronics, 2018,65(10): 8153-8162.
[2] Tao F., Cheng J., Qi Q. IIHub: an industrial internet-of-things hub toward smart manufacturing based on cyber-physical system. IEEE Transactions on Industrial Informatics, 2017, 14(5): 2271-2280.
[3] Wang Y., Zeng S., Yang Q. , et al. A new framework of electrical cyber physical systems. in Proc. ICIEA 2016, Hefei, China, June 2016, p. 1334-1339.
[4] Huang P., Wang Y., Yan G. Vulnerability analysis of electrical cyber physical systems using a simulation platform. in Proc. IECON 2017, Beijing, China, Nov. 2017, p. 489-494.
[5] Cai Y., Cao Y., Li Y., et al. Cascading failure analysis considering interaction between power grids and communication networks. IEEE Transactions on Smart Grid, 2016, 7(1): 530-538.
[6] Yaghmaee Moghaddam M. H., Leon-Garcia A. A fog-based internet of energy architecture for transactive energy management systems. IEEE Internet of Things Journal, 2018, 5(2): 1055-1069.
[7] Bindra A. Securing the power grid: protecting smart grids and connected power systems from cyberattacks. IEEE Power Electronics Magazine, 2017, 4(3): 20-27.

[8] Kurt M. N., Yılmaz Y., Wang X. Distributed Quickest Detection of Cyber-Attacks in Smart Grid. IEEE Transactions on Information Forensics and Security, 2018, 13(8): 2015-2030.

[9] Nespoli P., Papamartzivanos D., Mármol F. G. , et al. Optimal countermeasures selection against cyber attacks: a comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials, 2017, 20(2):1361-1396.

[10]Ren W., Wu J., Zhang X., et al. A stochastic model of cascading failure dynamics in communication networks. IEEE Transactions on Circuits and Systems II: Express Briefs,2018, 65(5): 632-636.

[11]Wei X., Gao S., Huang T., et al. Complex network based cascading faults graph for the analysis of transmission network vulnerability. IEEE Transactions on Industrial Informatics, in press.

[12]Bläsius T., Friedrich T. , Krohmer A. , et al. Efficient embedding of scale-free graphs in the hyperbolic plane. IEEE/ACM transactions on Networking, 2018, 26(2): 920-933.

[13]Qiu T., Liu X., Hu Q., et al. Community-aware data propagation with small world feature for internet of vehicles. IEEE Communications Magazine, 2018, 56(1): 86-91.

[14]Wang Q., Pipattanasompornm M., Kuzlu M., et al. Framework for vulnerability assessment of communication systems for electric power grids. IET Generation, Transmission & Distribution, 2016, 10(2): 477-486.

[15]Vellaithurai C., Srivastava A., Zonouz S., et al. CPINDEX: Cyber-physical vulnerability assessment for power-grid infrastructures. IEEE Transactions on Smart Grid, 2015, 6(2): 566-575.

[16]Srivastava A., Morris T., Ernster T., et al. Modeling cyber-physical vulnerability of the smart grid with incomplete information. IEEE Transactions on Smart Grid, 2013, 4(1): 235-244.

[17]Ji X., Wang B., Liu D., et al. Improving interdependent networks robustness by adding connectivity links[J]. Physica A: Statistical Mechanics and its Applications, 2016, 444:9-19.

[18]Cui P. , Zhu P., Wang K., et al. Enhancing robustness of interdependent network by adding connectivity and dependence links[J]. Physica A: Statistical Mechanics and its Applications, 2018, 497:185-197.

[19]Wang X., Cao J., Li R., et al. A preferential attachment strategy for connectivity link addition strategy in improving the robustness of interdependent networks[J]. Physica A: Statistical Mechanics and its Applications, 2017, 483:412-422.

[20]Chen Y., Li Y., Li W., et al. Cascading failure analysis of cyber physical power system with multiple interdependency and control threshold[J]. IEEE Access, 2018, 6: 39353-39362.

[21]Cai Y., Li Y., Cao Y., et al. Modeling and impact analysis of interdependent characteristics on cascading failures in smart grids[J]. International Journal of Electrical Power & Energy Systems, 2017, 89: 106-114.

[22]Sullivan J. E., Kamensky D. How cyber-attacks in Ukraine show the vulnerability of the U. S. power grid. Electricity Journal, 2017, 30(3): 30-35.

[23]Liu N., Yu X., Zhang J. Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid. Automation of Electric Power Systems, 2016, 40(6): 1-3.

[24]Yan J., Bo H., Sun Y. Integrated security analysis on cascading failure in complex networks. IEEE Transactions on Information Forensics and Security, 2014, 9(3): 451-463.

[25]Wei X., Zhao J. and Huang T., et al. A novel cascading faults graph based transmission network vulnerability assessment method. IEEE Transactions on Power Systems, 2018, 33(3): 2995-3000.

[26]Fan W., Liu Z., Hu P., et al. Cascading failure model in power grids using the complex network theory. IET Generation, Transmission & Distribution, 2016,10(15): 3940-3949.

[27]Khushalani S., Solanki J. M., Schulz N. N. Development of three-phase unbalanced power flow using PV and PQ models for distributed generation and study of the impact of DG models. IEEE Transactions on Power Systems, 2007, 22(3): 1019-1025.

[28]Duan C., Fang W., Jiang L., et al. Distributionally robust chance-constrained approximate AC-OPF with wasserstein metric. IEEE Transactions on Power Systems, 2018,33(5):4924-4936.

[29]Le Q., Panchal J. H. Building smaller sized surrogate models of complex bipartite networks based on degree distributions. IEEE Transactions on Systems, Man, and Cybernetics- Part A: Systems and Humans, 2012, 42(5): 1152-1166.

[30]Jamour F., Skiadopoulos S., Kalnis P. Parallel algorithm for incremental betweenness centrality on large graphs. IEEE Transactions on Parallel and Distributed Systems, 2018, 29(3): 659-672.