Tradeoff Between Robustness and Functionality in Cyber-Coupled Power Systems

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

***Abstract*—Robustness and functionality are conflicting requirements in cyber-coupled power systems. In general, a more tightly coupled power and cyber networks provides better functionality, but may degrade the robustness against attacks or failures. The way in which the power network is coupled with the cyber network is thus crucial to the design of robust cyber-coupled power networks while maintaining sufficient functionality. In this article, we classify coupling patterns according to two node-criticality metrics of the cyber network, i.e., node degree and node betweenness, and two node-criticality metrics of the power network, i.e., node degree and node capability. We use the relative coupling correlation coefficient to quantify the coupling pattern, and show that a coupled system with a lower relative coupling correlation coefficient has better robustness. A multiobjective problem is formulated and the Pareto optimal solutions are found to generate coupling patterns that give balanced robustness and functionality. Using a realistic physical power flow model, our results reveal possible tradeoff between functionality and robustness under different choices of criticality indexes.**

***Index Terms*—Complex networks, cyber-physical systems (CPS), power grids, robustness.**

I. Introduction

CYBER physical systems (CPS), comprising a suite of operational physical systems and some necessary intelligent cyber facilities, have become crucial infrastructural systems covering a wide spectrum of applications including communications, transportation, and power delivery. The study of CPS has recently emerged as a challenging research theme requiring cross-disciplinary efforts. The integration of smart devices like sensors and intelligent computational algorithms supports traditional physical systems with a significant upgrade of adaptability, autonomy, and efficiency [1]. Smart grids, which are specific implementations of CPS, consist of power apparatus such as generators, transformers, and transmission lines, connected with cyber-connected devices like phasor measurement units (PMU), wide area measurement systems, and advanced metering infrastructures (AMI) [2]. The use of cyber system facilities offers efficient monitoring and control of power systems [3], but at the same time creates loopholes that permit access by attackers who aim to disrupt the power system [4]. In the Ukrainian blackout event that occurred in December 2015 [5], a computer malware (called BlackEnergy) had penetrated to the computer networks that were connected to the power grid. Through infecting more computers and gaining unauthorized access, the hackers launched their attack by disconnecting circuit breakers in the power substations, resulting in an eight-hour long power outage. This incident has sounded alarm bells in the robustness of networked systems under cyber attacks.

Power systems coupled with cyber systems have recently been studied using a complex network approach. Specifically, a cyber-coupled power system is composed of a cyber network and a power network [6]–[8]. The former consists of interconnected cyber nodes, and the latter contains power substations connected by transmission lines. By using network-based approach, network properties including robustness and coupling patterns can be examined with quantitative analysis [9], [10].

Coupling pattern refers to the way in which different networks interact. Basically, in coupling two networks, the nodes in each network are first sorted by their importance. Then, the nodes sorted in ascending order in one network are connected to the nodes sorted in ascending or descending order in another network, resulting in an assortative or dissortative coupling pattern, respectively. In particular, assortative coupling patterns are more common than dissortative coupling patterns in real-life coupled networks, and an assortatively coupled network has more advantages than a dissortatively coupled one. For instance, it has been found [9] that port–airport systems exhibit characteristics of assortative coupling patterns. Also, Tan *et al.* [11] found that an assortative coupling pattern facilitates communication systems in mitigating congestion. In the study of China's power grids [12], a high degree of topological intersimilarity has been found between the power network and the coupled cyber network, which reveals to some extent the assortative nature in the way a pair of dependent nodes are coupled. To facilitate the function of controlling and monitoring power grids, high-degree cyber nodes are usually coupled with high-degree power nodes, as illustrated in the Italian grid [13]. These studies have highlighted the benefits of adopting an assortative coupling pattern in reducing the control cost and maintaining adequate functionality in cyber-coupled power systems. Furthermore, Xue *et al.* [14] have defined a measure called *node centrality correlation coefficient* to assess the interaction between a power grid and the supervising communication network, and revealed

Manuscript received June 22, 2020; revised November 13, 2020; accepted December 13, 2020. Date of publication January 11, 2021; date of current version March 24, 2022. This work was supported in part by the Hong Kong Research Grants Council under Grant GRF 152150/19E, in part by the City University of Hong Kong Grant 9380114, and in part by the National Natural Science Foundation of China under Grant 61803351. *(Corresponding author: Dong Liu.)*

Dong Liu and Chi K. Tse are with the Department of Electrical Engineering, City University of Hong Kong, Hong Kong (e-mail: adam.d.liu@connect.polyu.hk; chitse@cityu.edu.hk).

Xi Zhang is with the School of Automation, Beijing Institute of Technology, Beijing 100081, China (e-mail: xizhang@bit.edu.cn).

Digital Object Identifier 10.1109/JSYST.2020.3045597

the tight coupling between the two networks. Thus, under the condition of fixed control resources, coupling patterns play an important role in the functionality of coupled systems, and the assortative coupling pattern allows more functions to be facilitated in coupled networks. In today's power grid, efficient, reliable, and safe control is managed by a supervisory control and data acquisition (SCADA) system [15] which is assortatively coupled to the power network. In short, adopting an assortative coupling pattern is regarded as an effective strategy in designing a coupled system for the purpose of strengthening the functionality.

The strong dependence of network robustness on coupling patterns has motivated the study of adopting appropriate coupling patterns for enhancing the robustness of cyber-coupled power systems against cascading failure. The results obtained by Chen *et al.* [16] suggested that different categories of coupling patterns suppress cascading failure to different extents under various attack scenarios. Moreover, Rueda *et al.* [17] considered various interdependency matrices and identified the desirable properties that can effectively mitigate the impacts of targeted attacks on critical infrastructures.

It should be noted that much of the prior work adopted percolation theory to model failure spreading in interdependent networks, which omits the underlying physical processes. Hence, the conclusions drawn from these studies may not provide practically relevant suggestions to enhance the robustness of cyber-coupled power systems. To overcome the limitation of the network-based models, an engineering approach, considering the detailed physical operations, has been adopted to assessing the robustness of coupled systems focusing on examining the effect of cyber coupling on cascading failure in power systems [18] and the robustness of interdependent power grids and communication networks [19], [20]. Furthermore, most previous studies adopted a qualitative analysis of the correlations between robustness and coupling patterns, especially on assortative, random, and dissortative coupling patterns. In this article, we introduce a new parameter, called *relative coupling correlation coefficient*, to quantify coupling patterns. This parameter can be used to indicate the functionality of coupled systems, and study the effects of coupling patterns on the robustness of the coupled systems. We also propose four classes of coupling patterns with the consideration of two cyber node criticality metrics, i.e., node degree and node betweenness, and two power node criticality metrics, i.e., node degree and node capacity, for the purpose of ranking the node importance in the process of coupling power and cyber networks. Here, in a network, node degree refers to the number of nodes connected to a given node, and node betweenness refers to the frequency with which a given cyber node falls on the shortest path between other pairs of nodes. For the power network, node capacity is the maximum power below which a power node can work normally.

A network-based approach with due consideration of the physical process is adopted here to simulate cascading failure in cyber-coupled power systems. Results show that a higher *relative coupling correlation coefficient* gives a lower *robustness index* which indicates a less robust coupled system against cascading failure. Such finding is in contrary to the aforementioned related work [9], [11], [12], [16], [17] that ignore the physical processes. As the assortative coupling pattern can enhance functionality in cyber-coupled power systems, especially for better controllability and monitoring, a high *relative coupling correlation coefficient* should be preserved. In other words, in designing a cyber-coupled power system, two main objectives are often considered, namely, higher robustness and better functionality but they are obviously conflicting with each other. Thus, we formulate the identification of coupling patterns that achieve balanced objectives as a multiple-objective optimization problem and search for acceptable Pareto-optimal solutions by using the nondominated sorting genetic algorithm II (NSGA-II) [21]. The choice of node criticality has different implications on the robustness of coupled networks. For instance, choosing the node capacity as criticality index in power networks when optimizing coupling patterns has a negative influence on enhancing the robustness of coupled systems. These findings, however, cannot be obtained from pure network-based models which omit the essential physical operations. In practice, two crucial suggestions based on these findings could be considered in designing a cyber-coupled power system with expected functionality and robustness, namely, to assess such two concerned properties by using the proposed metrics and to enhance them by solving the multiobjective problem.

II. Model of Cyber-Coupled Power System

A cyber-coupled power system consists of a power network and a cyber network, as shown in Fig. 1. The power network, denoted as network A and shown as the bottom layer in Fig. 1, comprises a set of nodes (white squares) representing power substations and a set of links (solid lines) representing power transmission lines. A cyber network, denoted as network B in the upper layer, is composed of nodes (white circles) representing the cyber components, and links (dot-dash lines) representing the connections among cyber components. Moreover, the nodes in the power network and cyber network are also connected and their connections are shown by the vertical dash lines. In practice, a cyber node can access and control a power node when they are connected. In this article, the one-to-one connection style between power and cyber nodes is considered and each pair of coupled nodes is a "node pair" in the coupled network.

In this article, we take the cascading failure in the coupled system as a sequence of state transitions of node pairs. Three kinds of state transition are depicted in Fig. 1, including the malfunction of a power component, the infection of a cyber node due to malware spreading, and the launching of an attack on a power node by a cyber node.

Two main reasons for a power component to fail are considered in this model. First, a power component fails when it is in a subnetwork where there is no power generator. Second, a power component is prone to failure when it carries load that exceeds its capacity, and the probability of failure is expressed by the following state transition T_1:

$$T_1 : P[s_{A_i}(t + dt) = 1 \mid s_{A_i}(t) = 0] = \lambda_i(t)dt \qquad (1)$$

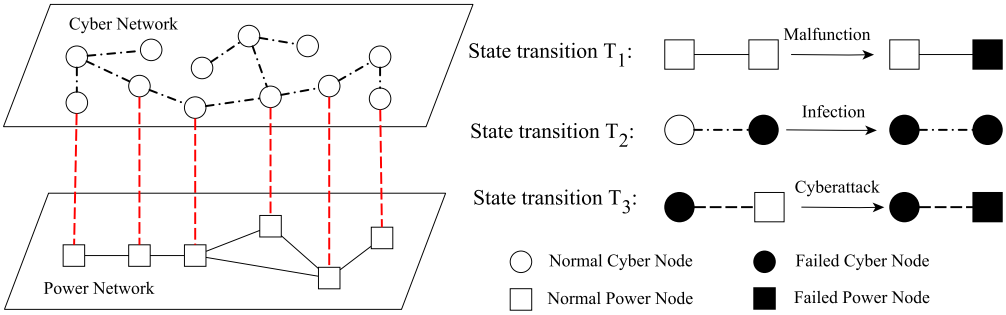


Fig. 1. Coupled network consisting of a cyber network and a power network, with state transitions showing infection of a cyber node, malfunction (overload tripping) of a power node and attack to a power node from a cyber node.

where $\lambda_i(t)$ is the tripping rate which is given by $\lambda_i(t) = a_i(L_i(t)/C(i) - 1)$ if the loading $L_i(t)$ is larger than the capacity $C_i(t)$ in the power component i, and is 0 otherwise. Moreover, the loading $L_i(t)$ is obtained from a dc power flow calculation model [22].

The malware diffusion in the cyber network is modeled by a stochastic process. In particular, a cyber node may be infected when its neighbor is infected, as described by state transition T_2

$$T_2 : P[s_{B_i}(t + dt) = 1 \mid s_{B_i}(t) = 0] = \mu_i(t)dt \qquad (2)$$

where $\mu_i(t)$ is the infection rate on cyber network which is given by $\mu_i(t) = \sum_{j\in\Omega_{Bi}} \beta_{ij}$. Specifically, Ω_{Bi} is the set of all infected neighbors of cyber node i and β_{ij} is the rate at which the infected cyber node j infects its neighbor node i.

When a power node is attacked by cyber malware, the probability of the power node being removed from the power network increases by a value $c_i(t)$ which corresponds to the attack strength. Moreover, if the effect of defense (protection) is considered, the probability of removing a power node due to its failure is reduced by a value $d_i(t)$. Thus, the state transition T_3 for failure due to a cyber attack is given by

$$\begin{aligned} T_3 : P[s_{A_i}(t + dt) = 1 \mid s_{A_i}(t) = 0] \\ = (\lambda_i(t) + c_i(t) - d_i(t))dt. \qquad (3) \end{aligned}$$

The cascading failure in a coupled system is simulated according to the flowchart shown in Fig. 2. After the initialization step, the process begins from a malware injection, which then spreads in the cyber network. In this stage, only state transition T_2 is executed. Once a cyber attack is launched, one of the three state transitions T_1, T_2, or T_3 is selected to be executed through determining (1) the instant when the next state transition occurs; and (2) the particular state transition to be executed in the current iteration. These two decisions are made by the stochastic method developed in a previous study [18]. It is noted that after each iteration, the states of the network will be updated, and the iteration continues until there is no further state transition.

In the coupled network-based model, the number of cyber nodes is larger than that of power nodes. The first step is to select the cyber nodes for connection with the power nodes using a one-to-one connection style. Here, we assume the selected cyber nodes can directly control the power nodes. The deployment of cyber facilities brings intelligent control and monitoring functions to modern grids. To implement automatic control, data such as voltage and current in power grids can be collected by sensors like power measurement units (PMU) and then the decision can be made by executing actions such as load shedding and optimal transmission switching. According to the specific types of functions [3], the nodes in a cyber network coupled with a power network can be categorized as data-collecting cyber nodes, decision-making cyber nodes, and others that play different roles such as data processing, data exchanging, etc. Distributing data-collecting and decision-making cyber nodes to appropriate locations in a cyber network aims at facilitating deployment of effective control to the coupled system [23].

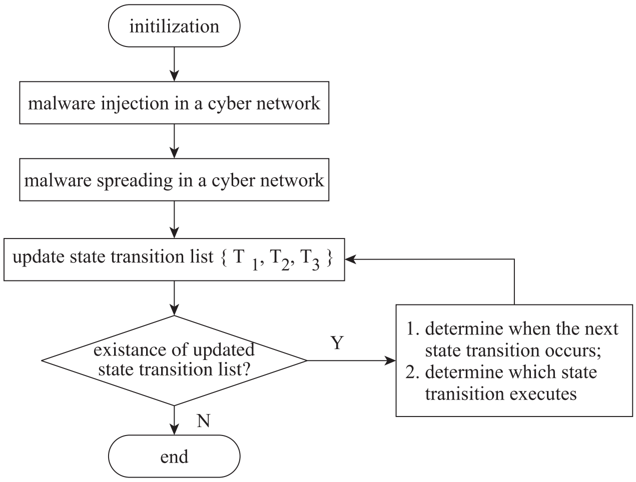
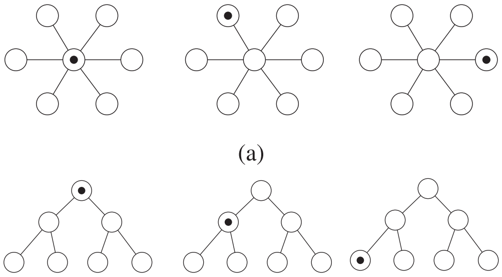

initilization
malware injection in a cyber network
malware spreading in a cyber network
update state transition list { T 1, T2, T3 }
existance of updated state transition list?
Y
N
1. determine when the next state transition occurs;
2. determine which state tranisition executes
end

Fig. 2. Flowchart of simulation of failure propagation in the coupled system.

The first main consideration in coupling a cyber network to a power network is to determine which decision-making cyber nodes are selected to be coupled with a power network. Borrowing the main idea from the controller placement problem in software defined networks [24], the criterion of selecting decision-making cyber nodes to be coupled with a power network is to minimize the packet propagation latency between decision-making cyber nodes and other nodes [24]. Here, the



(a)

(b)

Fig. 3. Average propagation latency of (a) star network when one decision-making cyber node (with a dot inside) is placed in three different locations. (b) Tree network when one decision-making cyber node (with a dot inside) is placed in three different locations.

average propagation latency, denoted by ϵ, is defined as

$$\epsilon = \frac{1}{N-K} \sum_{a \in A \setminus A_c} d(a, A_c) \tag{4}$$

where A_c is the set of decision-making cyber nodes, $A \setminus A_c$ refers to the set of cyber nodes other than the decision-making cyber nodes, K is the number of decision-making cyber nodes, and $d(a, A_c)$ represents the shortest path length between a cyber node a in the set of $A \setminus A_c$ to its nearest decision-making cyber node. A diagrammatic explanation is given in Fig. 3 for the proposed metric ϵ. Two basic topologies of communication networks are exemplified here, namely, star and tree network topologies. For the star network, $\epsilon = (1/6) \times (1+1+1+1+1+1) = 1$ (left), $\epsilon = (1/6) \times (1+2+2+2+2+2) = 11/6$ (middle), and $\epsilon = (1/6) \times (1+2+2+2+2+2) = 11/6$ (right). For the tree network, $\epsilon = (1/6) \times (1+1+2+2+2+2) = 10/6$ (left), $\epsilon = (1/6) \times (1+1+1+2+3+3) = 11/6$ (middle), and $\epsilon = (1/6) \times (1+2+2+3+4+4) = 16/6$ (right). It is noted that the shortest packet propagation latency is found in the left scenario for both network cases. For a given cyber network, the position of a node serving as a decision-making node significantly affects the value of ϵ. An appropriate placement (central position in these examples) of the decision-making node can lead to a higher efficiency because of the small value of ϵ, which is also a critical requirement in designing communication networks for modern smart grids [25]. In reality, a decentralized modular device network, such as the one adopted in Japanese grids, can exhibit low latency and delay variation in power system monitoring, and can therefore provide adaptive protection and emergency control to prevent large blackout and localize disruption [26].

III. Coupling Patterns

The coupling pattern is the way in which the cyber and power nodes are connected. The choice of the coupling pattern has a profound impact on the robustness of coupled networks. In particular, it has been found that a *higher intersimilarity* increases the robustness of a coupled network. One specific intersimilarity metric called *inter degree–degree correlation* (IDDC) has been introduced by Parshani *et al.* [9], and given as $r = \frac{1}{\sigma_q^2} \sum_{jk} jk(e_{jk} - p_j p_k)$. Specifically, p_j and p_k are the degree distributions of two networks in a coupled system and e_{jk} is the joint probability that an interdependency link becomes the connection between the node in one network with degree j and the node in the other network with degree k. The correlation r can be written as a form of associative mixing coefficient

$$r = \frac{M^{-1}\sum_i j_i k_i - [M^{-1}\sum_i \frac{1}{2}(j_i + k_i)]^2}{M^{-1}\sum_i \frac{1}{2}(j_i^2 + k_i^2) - [M^{-1}\sum_i \frac{1}{2}(j_i + k_i)]^2} \tag{5}$$

where j_i and k_i are the degrees of the nodes in two individual networks at the end of the ith interdependent link, with $i = 1, 2, \ldots, M$. Moreover, if networks A and B have the same degree distribution, r is between –1 and +1. Also, a large value of r corresponds to an assortative coupling pattern, i.e., high degree nodes in A are connected to high degree nodes in B. On the other hand, a small (negative) value of r corresponds to a dissortative coupling pattern, i.e., high degree nodes in A are connected to low degree nodes in B. Fig. 4 illustrates the coupling patterns diagrammatically. In particular, the left scenario corresponds to an assortative coupling with a positive ρ, the middle scenario shows an intermediate coupling between assortative and dissortative coupling patterns, and the right scenario corresponds to a dissortative coupling with a negative ρ.

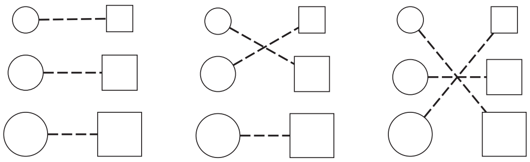


Fig. 4. Illustration of relative coupling correlation coefficient ρ.

In our study of cyber-coupled power systems, apart from using node degrees, we consider a few other network-based metrics for describing node criticality. Here, we characterize the coupling pattern by extending the IDDC coefficient to an inter criticality–criticality correlation coefficient. This new metric, called *relative coupling correlation coefficient*, is defined as

$$\rho = \frac{M^{-1}\sum_m I'_{Am} I'_{Bm} - [M^{-1}\sum_m \frac{1}{2}(I'_{Am} + I'_{Bm})]^2}{M^{-1}\sum_m \frac{1}{2}(I'^2_{Am} + I'^2_{Bm}) - [M^{-1}\sum_m \frac{1}{2}(I'_{Am} + I'_{Bm})]^2} \tag{6}$$

where I'_{Am} and I'_{Bm} are the normalized node criticality metrics of two nodes in the two interconnected networks, respectively, when they are connected by edge m. As explained before, the existence of interconnected edge m connecting cyber and power nodes implies that the cyber node can take a malicious action against its coupled power node.

Specifically, the normalized node criticality metrics for network A is

$$I'_A = \frac{I_A - \min(I_A)}{\max(I_A) - \min(I_A)} \tag{7}$$

where I_A is a node criticality metric in the power network, which indicates the importance of the power node. Likewise, the normalized node criticality metrics for network B is

$$I'_B = \frac{I_B - \min(I_B)}{\max(I_B) - \min(I_B)} \tag{8}$$

where I_B is a node criticality metric in the cyber network, which indicates the importance of the cyber node.

In connecting the pairs of interdependent nodes from the two networks, we first sort the cyber and power nodes by their node criticality. In Fig. 4, the node with a larger size means the node is of higher criticality. Then, the sorted cyber and power nodes are connected in different orders. As shown in the left case of Fig. 4, connecting the sorted cyber and power nodes in an ascending order leads to an assortative coupling pattern, i.e., the cyber nodes with higher node criticality are connected with the power nodes with higher node criticality. In the contrary, connecting the sorted cyber and power nodes in a descending order implies that the cyber nodes with lower node criticality are connected with the power nodes with higher node criticality, which is a dissortative coupling pattern, as shown in the right case of Fig. 4. These two types of coupling patterns are quantified as a positive ρ and a negative ρ, respectively. Besides these two patterns, building dependent pairs of nodes in different orders can be quantified by the relative coupling correlation coefficient, as given by (6).

For node criticality, it is proposed to evaluate how critical a node takes a role in a network including answering a question that which nodes are best connected to other nodes or exhibit the largest influence in the network. Here, we take *node centrality* as the measurement of node criticality [27]. Specifically, a node located in the most central position serves as an active and efficient component for data transmission in the cyber network [28]. Thus, a cyber node with higher centrality can be identified as a cyber component which exhibits a stronger capability of controlling a power component in a cyber-coupled power network and thus helps enhance the system's functionality. In this article, we focus on two main node centrality metrics, namely, *node degree* and *node betweenness* for assessing the node importance in cyber networks. Also, topological properties take an essential role in identifying critical components in power grids for the purpose of enhancing vulnerability analysis [29]. For power networks, based on previous study on network robustness [30], we choose *node degree* and *node capacity* as the measure of node criticality.

In this article, several classes of coupling patterns corresponding to different combinations of adoption of node criticality metrics in power and cyber networks can be considered. In particular, we consider four classes of power-to-cyber coupling patterns, namely: 1) *degree-to-degree (d2d)*; 2) *degree-to-betweenness (d2b)*; 3) *capacity-to-degree (c2d)*; and 4) *capacity-to-betweenness (c2b)*.

IV. Robustness

Robustness of a system reveals the capability of a system in withstanding an unexpected event without degrading its performance. In other words, when such an unexpected perturbation happens, a larger damage occurring in a system implies that a system is more vulnerable and hence less robust. In this article, we adopt the definition of vulnerability introduced by Schneidera *et al.* [31], which essentially considers the size of the largest affected component during all possible malicious attack. Similarly, to assess the *vulnerability* of a cyber-coupled power system against cascading failure due to a cyber attack, we consider the extent of failure in the power network under various scales of malware infection in a cyber network, which can be written as

$$V = \frac{1}{N_S} \sum_{s \in S} S_{\mathrm{PN}} \mid_{S_{\mathrm{CN}} = n_s} \tag{9}$$

where S_{PN} is the extent of cascading failure in the power network (number of failed power components), S_{CN} is the extent of infection in the cyber network (number of infected cyber nodes), S is a set of N_S infected cyber subnetworks, and in each cyber subnetwork s, n_s nodes have been infected. For instance, $n_s = 10$ means that there have been ten infected cyber nodes. Under the circumstance when n_s cyber nodes are infected, the size of cascading failure in power networks is recorded as $S_{\mathrm{PN}} \mid_{S_{\mathrm{CN}} = n_s}$. Through calculating the average value, the vulnerability of a cyber-coupled power system can be assessed. A larger value of this measure indicates a more severe cascading failure as a result of a cyber attack. For instance, when the sequence of S_{CN} (number of infected cyber nodes) is 10, 20, and 30, the sequence of S_{PN} (number of failed power nodes) recorded in two cyber-coupled power systems with coupling patterns CCPS1 and CCPS2 are 10, 20, 30 and 15, 25, 35, respectively. In this case, the *vulnerability* of CCPS1 ($V = 20$) is lower than that of CCPS2 ($V = 25$). Furthermore, a *robustness* index can be transformed from the vulnerability measurement

$$R = 1 - \frac{V}{N_A} \tag{10}$$

where N_A is the size of a power network. Through normalization, the value of R is made to fall between 0 and 1. A larger value of R implies that a power system can survive with a smaller fraction of failed nodes due to cyber attacks.

A. Case Studies

1) Case 1: In this first case study, the coupled system is composed of an IEEE 30-bus power system [32] and a cyber network represented by a synthesized 1000-node scale-free network. We set the basic unit failure rate of a power component tripped by power overloading $a_i = 0.035\,\mathrm{s}^{-1}$ and the infection rate $\beta_{i,j} = 0.0175\,\mathrm{s}^{-1}$. Moreover, we consider the attack strength is larger than the defense strength, so $c_i = 0.2\,\mathrm{s}^{-1}$ and $d_i = 0.1\,\mathrm{s}^{-1}$. The percentages of the failed nodes in cyber and power networks, namely PFCN(t) and PFPN(t), are recorded for reflecting the growing trend of cascading failure. In the following experiment, we select the decision-making cyber nodes in two steps: 1) A large number of sets of nodes including N_A (the number of nodes in a given power system) cyber nodes are randomly chosen from a given cyber network. 2) For each set, the value of ϵ is calculated, and if ϵ is equal to the value under consideration, the cyber nodes in the set are chosen as the decision-making cyber nodes.

Fig. 5 shows six failure propagation profiles in the cyber-coupled power system with six coupling patterns, which can be

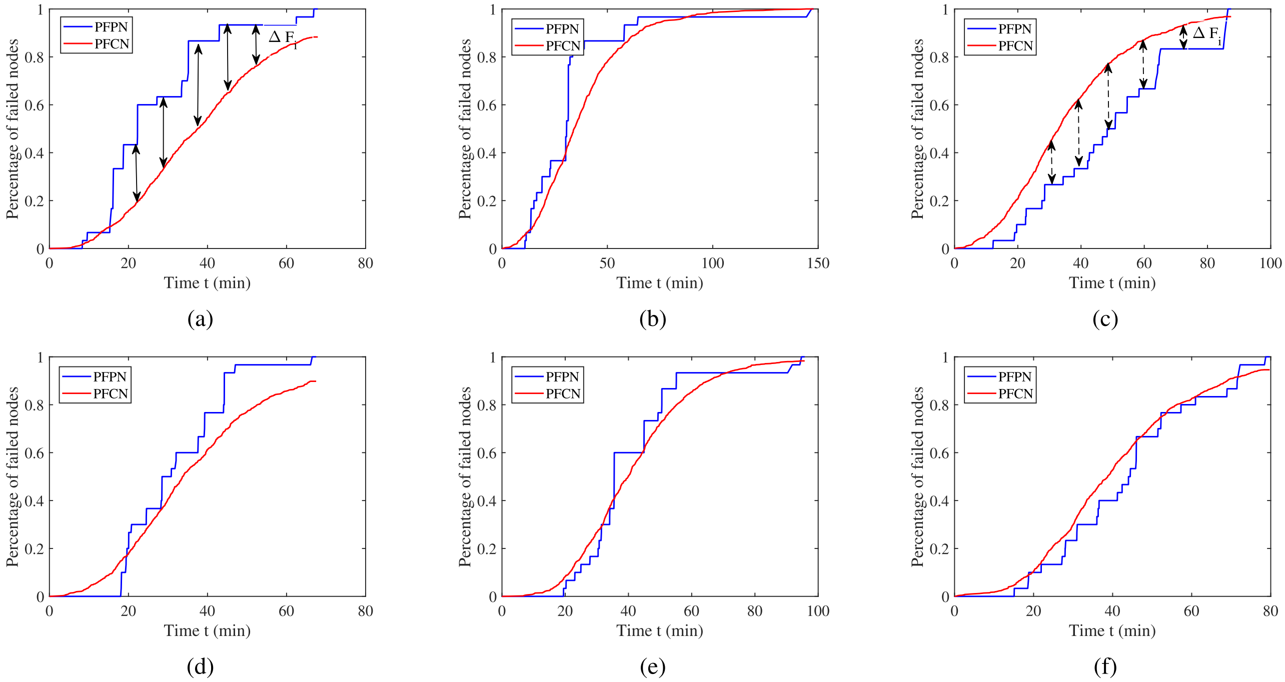


Fig. 5. Failure propagation in coupled systems with the adoption of six coupling patterns. Evenly distributed control scenario. (a) Assortative. (b) Random. (c) Dissortative coupling patterns. Unevenly distributed control scenario. (d) Assortative. (e) Random. (f) Dissortative coupling patterns.

divided into two scenarios based on the selection of decision-making cyber nodes, namely, an evenly distributed control scenario and an unevenly distributed control scenario. In the evenly distributed control scenario, the decision-making nodes are selected by assigning a small value of ϵ, which corresponds to shorter distances of data transmission from other cyber nodes to the decision-making nodes. Thus, the control action can be performed in a short response time. Conversely, if the decision-making cyber nodes are chosen based on assigning a large value of ϵ, they might receive data from other nodes and then make the control decision with high latency.

For the evenly distributed control scenario, three coupling patterns, namely, assortative, random, and disassortative, as described in Fig. 4, are adopted to simulate cascading failure. The failure propagation profiles of the cyber and power networks are presented in Fig. 5(a)–(c). It can be seen in Fig. 5(a) that PFCN(t) is below PFPN(t). In Fig. 5(b), the two failure propagation profiles are closer compared with the case shown in Fig. 5(a). Different from assortatively coupled two networks, PFCN(t) is above PFPN(t). The change of the relative positions of the two profiles in Fig. 5(a)–(c) indicates that if the cyber and power networks are coupled dissortatively, the attacker needs to infect more cyber nodes in order to cause a large-scale power outage, compared to the case of asortatively coupling the cyber and power networks. A similar phenomenon can be observed in Fig. 5(d)–(f) for the unevenly distributed control scenario.

To further illustrate the vulnerability of the coupled system, an intuitive parameter ΔF is defined based on the distance of the two profile curves of failure in power and cyber networks, as shown in Fig. 5(a) and (c). The values of ΔF_i are sampled at various time points, and the mean value $\overline{\Delta F}$ is calculated.

TABLE I
MEAN VALUE OF THE DISTANCE OF THE FAILURE PROPAGATION PROFILES OF CYBER AND POWER SYSTEMS $\overline{\Delta F}$ DUE TO CYBER ATTACKS

	Assortative	Random	Dissor- tative
Evenly distributed control scenario (low ϵ)	0.11	0.05	0.03
Unevenly distributed control scenario (high ϵ)	4.05×10^{-3}	1.41×10^{-4}	-0.06

Table I compares $\overline{\Delta F}$ among the six aforementioned scenarios through averaging the results over 1000 simulation runs. We found that the values in the evenly distributed control scenarios are higher than those in the unevenly distributed control scenarios. In summary, we have the following results.

1) A dissortative coupling pattern leads to a more robust coupled system.
2) Decision-making cyber nodes selected based on a smaller ϵ make the coupled system more robustness.

Thus, to avoid cascading failure in a cyber-coupled power system due to cyber attacks, it is advisable to select decision-making cyber nodes based on an unevenly distributed control strategy and dissortatively coupled power and cyber systems.

2) Case 2: We consider a cyber system realized by a Gnutella peer-to-peer network [33] containing 6301 nodes. This network is coupled with the UIUC-150 power system [32], forming a cyber-coupled power system. To examine the effect of the

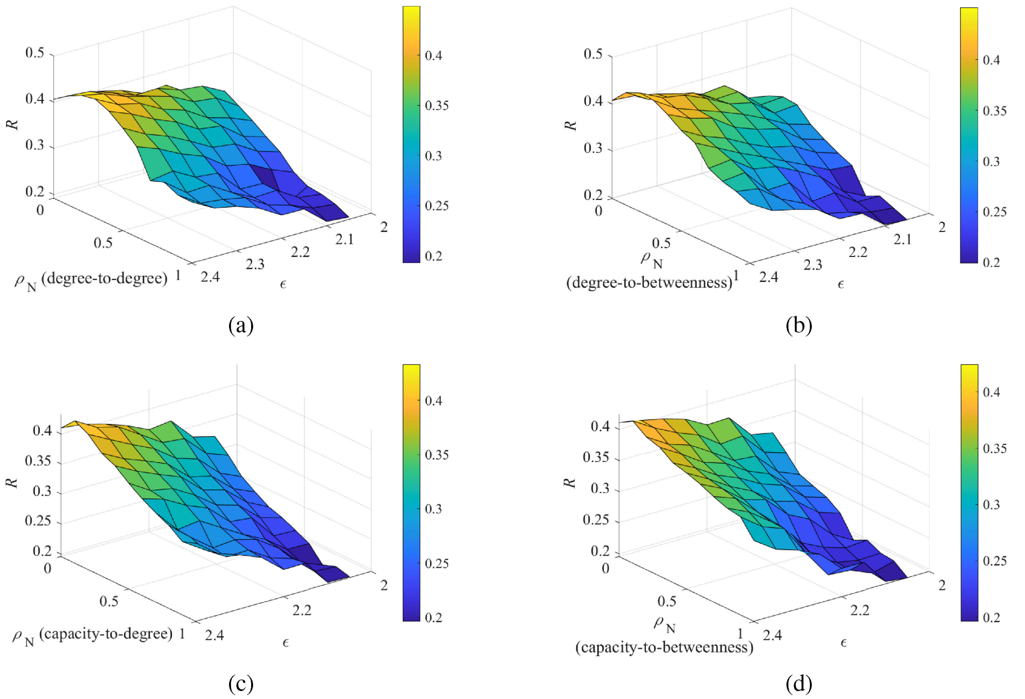


Fig. 6. Effect of relative coupling correlation coefficient and average propagation latency on the robustness of cyber-coupled power systems. Four combinations of adoption of criticality indices are considered, namely, (a) degree-to-degree, (b) degree-to-betweenness, (c) capacity-to-degree, and (d) capacity-to-betweenness.

average propagation latency ϵ and the relative coupling correlation coefficient ρ on the robustness of cyber-coupled power systems, experiments are conducted as follows.

1) *Step I:* For a given cyber network, decision-making nodes are identified, and a few values of ϵ are obtained based on different choices of decision-making nodes.
2) *Step II:* Based on the selected decision-making cyber nodes, various coupling patterns corresponding to different values of ρ can be realized for coupling the cyber network to the power network.
3) *Step III:* Cascading failure simulation is performed for each coupling pattern and the robustness index R can be found by analyzing the simulation results. In particular, the numbers of failed power components are recorded when $10\%, 20\%, \ldots, 100\%$ cyber nodes in the cyber network are infected, and the value of V can be calculated according to (9). The value of R can then be found from (10) accordingly. It is noted that the attack from the cyber network to the power network is launched when the malware starts to infect the cyber network.

Fig. 6 shows the effect of coupling patterns on the robustness of cyber-coupled power systems against cascading failure. For ease of comparison, a normalized ρ, defined as $\rho_{\mathrm{N}} = (\rho - \rho_{\min})/(\rho_{\max} - \rho_{\min})$, is used. According to Fig. 6(a), with the same value of ρ_{N}, e.g., $\rho_{\mathrm{N}} = 1$, r decreases from 0.2–0.15. Moreover, given the same value of ϵ, namely, $\epsilon = 2.4$, the value of r is also decreasing from 0.4 to 0.2. Furthermore, we consider four different combinations of adoption of criticality metrics in power and cyber networks, i.e., degree-to-degree, degree-to-betweenness, capacity-to-degree, and capacity-to-betweenness, which are depicted in Fig. 6(a)–(d). In general, the surfaces shown in Fig. 6(c) and (d) are flatter than those shown in Fig. 6(a) and (b). The difference implies that taking node capacity as the node criticality in power networks leads to less variation for the choice of the decision-making cyber nodes and lower sensitivity of the coupling pattern on the robustness of cyber-coupled power systems. Referring to these diagrams, where a lighter color refers to a higher robustness index, two key observations can be made.

1) A smaller average propagation latency leads to a less robust cyber-coupled power system.
2) For a given average propagation latency, a larger relative coupling correlation coefficient leads to a less robust cyber-coupled power system.

The first observation is clearly consistent with the fact that the decision-making cyber nodes selected based on a smaller average propagation latency are more likely to be infected by malware in cyber networks. In other words, under the condition of the same number of cyber nodes being infected, more decision-making cyber nodes are infected when the average propagation latency is smaller. A small average propagation latency thus intensifies the cascading failure in power grids. The second observation, however, does not agree with some previously reported work [9], [12] which has demonstrated that assortative coupling patterns contribute to improving the robustness of coupled networks. In our simulation, we take into consideration the effects of power overloading based on a physical power flow model, contagion, and interdependence between power grids and cyber networks on failure propagations in coupled systems. The results indicate that the assortative coupling pattern degrades the robustness of coupled systems.

V. Robustness and Functionality Tradeoff

Adopting assortative coupling patterns is highly desirable in cyber-coupled power systems. One of the major reasons for the widespread adoption of assortative coupling patterns is to ensure the high reliability of controlling the power network with low control cost. In particular, a higher relative coupling correlation coefficient indicates that high-criticality power nodes tend to be connected to high-criticality cyber nodes for ensuring high reliability and efficient operation because the high-criticality cyber nodes can be regarded to be more capable in controlling high-criticality power nodes. On the one hand, an assortative coupling pattern allows more functions to be facilitated in coupled networks under the condition of fixed control resources. On the other hand, if low-criticality cyber nodes are coupled with high-criticality power nodes, which is regarded as dissortative coupling, the control cost is increased because more cyber nodes will be utilized to support the control functions in the power nodes. Thus, the functionality of the coupled systems including some intelligent control functions will be degraded unless a higher control cost is paid. In summary, a high relative coupling correlation coefficient is desirable for better control and monitoring, while a high robustness index is also important. Thus, a tradeoff exists in the design of coupling patterns to strike a balance between functionality and robustness.

In the following we formulate a multiobjective problem to seek coupling patterns that achieve balanced objectives. Then, Pareto-optimal solutions are found by using the NSGA-II [21].

A. Problem Formulation

The goal of the multiobjective optimization is to find a solution in optimizing different objectives that are contradictory to each other. The ultimate aim of solving a multiobjective optimization problem is to obtain an optimal Pareto front containing possible solutions. As discussed before, obtaining an appropriate coupling pattern is a two-objective optimization problem. The first objective is to maximize the robustness of cyber-coupled power systems against cascading failure, which is described based on robustness index R

$$\max(R). \tag{11}$$

Moreover, to achieve an assortative coupling pattern in a cyber-coupled power system (for better control and monitoring functionalities), the second objective is to maximize the relative coupling correlation coefficient

$$\max(\rho). \tag{12}$$

Other minor constraints like geographical factors [34] are not considered in this article.

Genetic algorithms are effective approaches for solving multiobjective optimization problems. The NSGA-II algorithm [21] is adopted to search for Pareto-optimal solutions. In this algorithm, individuals in the population have different chromosomes that represent different permutations of the indices of cyber nodes. Combined with a fixed permutation of the indices of power nodes, one specific permutation of the indices of cyber nodes corresponds to a coupling pattern. Based on a given coupling pattern, two objectives, i.e., maximizing R and maximizing ρ, which are regarded as fitnesses in the algorithm. The population size and generation number are set as 20 in this article. Also, the mutation probability and crossover probability are 0.1 and 0.9, respectively.

B. Pareto-Optimal Solutions

A Pareto-optimal set contains a set of solutions in which no solution dominates over others. In other words, optimizing one objective may lead to a certain amount of sacrifice of other objectives when comparing one Pareto-optimal solution with another. In our case, the Pareto-optimal set provides a set boundary curves on the 2-dim ρ–R plane that shows how R can be traded for ρ when delivering optimal performance. As will be shown below, each curve is monotonically decreasing and convex downward, indicating that R can only be enhanced at the expense of weakened ρ and *vice versa*.

The Pareto-optimal solutions are obtained by using NSGA-II algorithm and four combinations of the adoption of criticality indices are considered in obtaining different values of the relative coupling correlation coefficient, as depicted in Fig. 7(a)–(c). Here, we can see that at the same value of average propagation latency ϵ, increasing the robustness index R makes a reduction of the relative coupling correlation coefficient, which is consistent with the conclusion in Section IV-A2. However, applying NSGA-II algorithm in this article generates preferred results in optimizing coupling patterns with balanced objectives. In particular, the Pareto-optimal solutions offer coupling patterns that can achieve higher robustness with yet adequate coupling assortativity. Tradeoff regions between robustness and coupling assortativity of the coupled system are shown in Fig. 7, where Pareto-optimal solutions are given at varied average propagation latency. In the case of degree-to-degree coupling shown in Fig. 7(a), the solutions (circle markers) have values of R from 0.2 to 0.4, ranging from a ρ_{N} of 0.2–1 when $\epsilon = 2.05$. In the case of $\epsilon = 2.35$, the range of the value of R in the solutions (hexagram markers) is from 0.33 to 0.47 corresponding to the consistent range of ρ_{N} in the above case. Such comparison reveals that increasing the value of ϵ enlarges the range of robustness index while keeping the same range of coupling assortativity. This change can be observed in Fig. 7(a)–(d), which implies that a larger value of ϵ can offer a preferred set of Pareto-optimal solutions which have larger values of ρ_{N} for a given value of R.

The Pareto-optimal solutions under four combinations of the adoption of criticality indices in power and cyber networks are shown in Fig. 8(a)–(d), where four values of ϵ are considered. From these results, when node capacity is chosen as the criticality index of power nodes, regardless of the choice of criticality index in cyber networks, the effectiveness of obtaining a coupled system with high robustness and high coupling assortativity is the poorest. It is noted that the capacity information is not obtainable without due consideration of the physical power flow process in network-based models.

Finally, a few examples may help clarify the use of the Pareto-optimal bounds. Suppose a coupled system with high robustness, say $R = 0.35$, is desired. From Fig. 8(a), the smallest

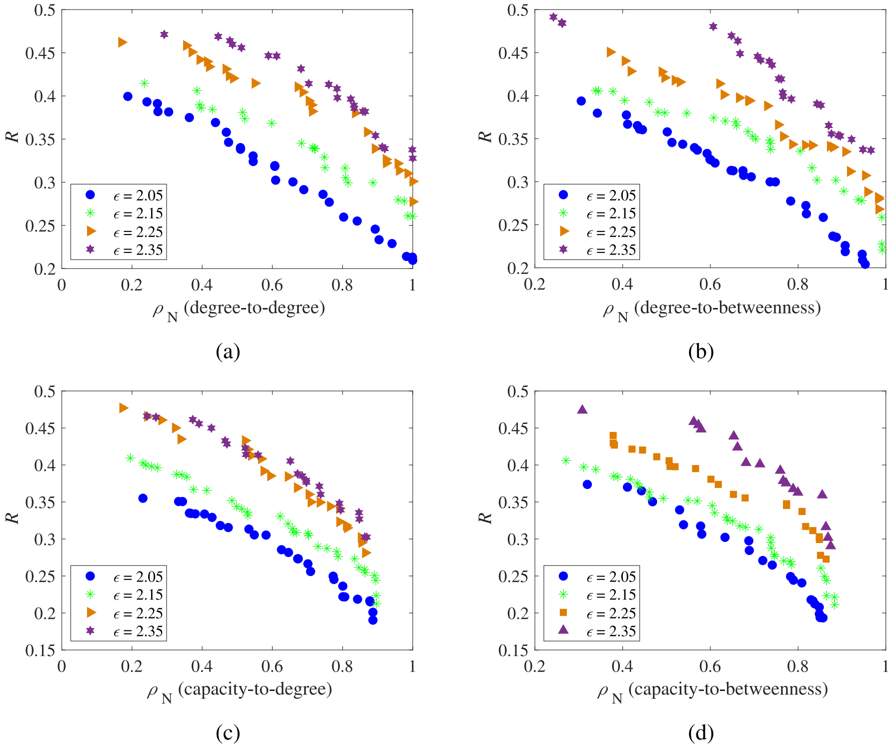


Fig. 7. Pareto-optimal bounds obtained by using NSGA-II algorithm showing achievable relative coupling correlation coefficient and robustness index. Four combination of the adoption of criticality index are considered. (a) Degree-to-degree. (b) Degree-to-betweenness. (c) Capacity-to-degree. (d) Capacity-to-betweenness. In each case, decision-making nodes are selected by fixing four values of average propagation latency.

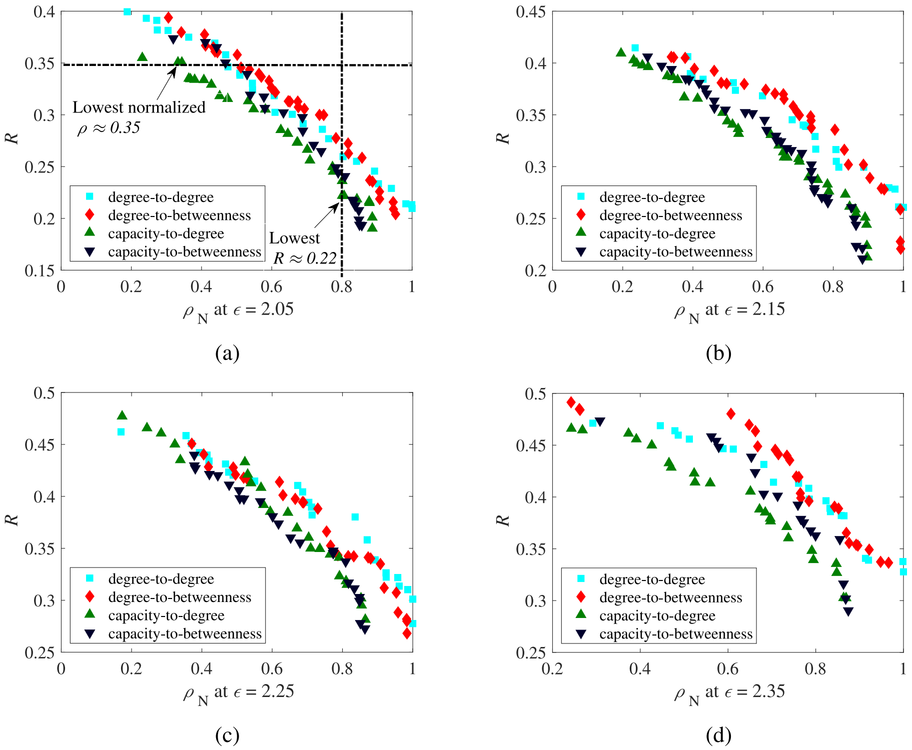


Fig. 8. Pareto-optimal bounds obtained by using an NSGA-II algorithm showing achievable relative coupling correlation coefficient and robustness index. Four combinations of the adoption of criticality indices are considered in obtaining different values of the relative coupling correlation coefficient under the condition of four values of average propagation latency. (a) $\epsilon = 2.05$. (b) $\epsilon = 2.15$. (c) $\epsilon = 2.25$. (d) $\epsilon = 2.35$.

value of ρ_{N} is identified as around 0.35 if *capacity-to-degree* coupling is adopted. For a coupled system aiming at a higher coupling assortativity, e.g., $\rho_{\mathrm{N}} = 0.8$, the lowest obtainable value of R is around 0.22, when adopting *capacity-to-degree* coupling. Similarly, when *capacity-to-betweenness* coupling is adopted, the solutions given in the Pareto-optimal sets are not the desired choices. However, adopting *degree-to-degree* or *degree-to-betweenness* coupling can achieve a better Pareto-optimal solution set that helps coupled systems maintain higher robustness without losing much gain of functionality. Thus, choosing node capacity as the criticality index of power nodes is unlikely to achieve a good balance between higher robustness and better functionality.

VI. Conclusion

Smart grids, regarded as cyber-physical systems, are vital infrastructures demanding high robustness. With the integration of intelligent monitoring and control functions provided by cyber networks, a cyber-coupled power system becomes vulnerable to cyber attacks and severe power outage might be caused. In this article, we reveal the role of coupling patterns in determining the functionality and robustness of coupled systems, and we aim to track coupling patterns by considering the tradeoff between the functionality and robustness. In particular, we introduce a parameter called average propagation latency for selection of decision-making cyber nodes to be coupled with power nodes. Another parameter called relative coupling correlation coefficient is proposed to quantify the coupling pattern. Results show that a smaller average propagation latency or a larger relative coupling correlation coefficient reduces the robustness of cyber-coupled power systems. Moreover, increasing the relative coupling correlation coefficient makes the coupling assortativity higher and hence facilitates better control and monitoring functionality, while a higher coupling assortativity makes the network more vulnerable. Thus, we formulate the problem of designing coupling patterns as a multiobjective problem, and use an evolutionary algorithm to search for Pareto-optimal solutions. Combining physical power flow models and network-based methods, we show that choosing node capacity as the criticality index in a power network for perusing coupling patterns under expectation will limit the effectiveness of improving network robustness. Future work will focus other constraints in implementing coupling patterns in real-world cyber-coupled power systems.

References

[1] K. Kim and P. R. Kumar, “Cyber-physical systems: A. perspective at the centennial,” *Proc. IEEE*, vol. 100, no. 5, pp. 1287–1308, May 2012.

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

[3] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, “Modeling of future cyber-physical energy systems for distributed sensing and control,” *IEEE Trans. Syst., Man, Cybern. A., Syst., Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[4] K. Wang *et al.*, “A survey on energy Internet: Architecture, approach, and emerging technologies,” *IEEE Syst. J.*, vol. 12, no. 3, pp. 2403–2416, Sep. 2018.

[5] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the Ukrainian power grid,” Mar. 2016. [Online]. Available: https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

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

[7] M. Zeraati, Z. Aref, and M. A. Latify, “Vulnerability analysis of power systems under physical deliberate attacks considering geographic-cyber interdependence of the power system and communication network,” *IEEE Syst. J.*, vol. 12, no. 4, pp. 3181–3190, Dec. 2018.

[8] D. Liu and C. K. Tse, “Cascading failure of cyber-coupled power systems considering interactions between attack and defense,” *IEEE Trans. Circuits Syst. I. Reg. Papers*, vol. 66, no. 11, pp. 4323–4336, Nov. 2019.

[9] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, and S. Havlin, “Inter-similarity between coupled networks,” *Europhysics Lett.*, vol. 92, no. 6, Jan. 2010, Art. no. 68002

[10] C. D. Brummitt, R. M. D’Souza, and E. A. Leicht, “Suppressing cascades of load in interdependent networks,” *Proc. Nat. Acad. Sci. USA*, vol. 109, no. 12, pp. E680–E689, Dec. 2012.

[11] F. Tan, J. Wu, Y. Xia, and C. K. Tse, “Traffic congestion in interconnected complex networks,” *Phys. Rev. E*, vol. 89, Jun. 2014, Art. no. 62813.

[12] X. Ji *et al.*, “Will electrical cyber-physical interdependent networks undergo first-order transition under random attacks?” *Phys. A: Statist. Mech. Appl.*, vol. 460, pp. 235–245, Oct. 2016.

[13] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola, “Modelling interdependent infrastructures using interacting dynamical models,” *Int. J. Crit. Infrastructures*, vol. 4, no. 1/2, pp. 63–79, Jan. 2008.

[14] Y. Xue, M. Ni, J. Yu, J. Hu, and W. Yu, “Study of the impact of communication failures on power system,” in *Proc. IEEE Power Energy Soc. Gen. Meeting*, pp. 1–5, Jul. 2015.

[15] “Supervisory control and data acquisition (SCADA) systems,” Oct. 2004. [Online]. Available: http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/gheyreboomi/mabanisyscontrlsanati/SCADA%20Basics%20-%20NCS%20TIB%2004-1.pdf

[16] L. Chen, D. Yue, C. Dou, Z. Cheng, and J. Chen, “Robustness of cyber-physical power systems in cascading failure: Survival of interdependent clusters,” *Int. J. Elect. Power Energy Syst.*, vol. 114, Jan. 2020, Art. no. 105374.

[17] D. F. Rueda and E. Calle, “Using interdependency matrices to mitigate targeted attacks on interdependent networks: A. case study involving a power grid and backbone telecommunications networks,” *Int. J. Crit. Infrastructure Prot.*, vol. 16, pp. 3–12, Mar. 2017.

[18] X. Zhang, D. Liu, C. Zhan, and C. K. Tse, “Effects of cyber coupling on cascading failures in power systems,” *IEEE J. Emerg. Sel. Top. Circ. Syst.*, vol. 7, no. 2, pp. 228–238, Jun. 2017.

[19] Z. Chen, J. Wu, Y. Xia, and X. Zhang, “Robustness of interdependent power grids and communication networks: A complex network perspective,” *IEEE Trans. Circuits Syst. II, Express Briefs*, vol. 65, no. 1, pp. 115–119, Jan. 2018.

[20] X. Gao, M. Peng, C. K. Tse, and H. Zhang, “A stochastic model of cascading failure dynamics in cyber-physical power systems,” *IEEE Syst. J.*, vol. 14, no. 3, pp. 4626–4637, Sep. 2020.

[21] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, “A fast and elitist multiobjective genetic algorithm: NSGA-II,” *IEEE Trans. Evol. Comput.*, vol. 6, no. 2, pp. 182–197, Apr. 2002.

[22] X. Zhang and C. K. Tse, “Assessment of robustness of power systems from a network perspective,” *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 5, no. 3, pp. 456–464, Sep. 2015.

[23] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on smart grid communication infrastructures: Motivations, requirements and challenges,” *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 5–20, Feb. 2013.

[24] B. Heller, R. Sherwood, and N. McKeown, “The controller placement problem,” in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, Aug. 2012, pp. 7–12.

[25] W. Wang, Y. Xu, and M. Khanna, “A survey on the communication architectures in smart grid,” *Comput. Netw.*, vol. 55, no. 15, pp. 3604–3629, Oct. 2011.

[26] Y. Serizawa, E. Ohba, and M. Kurono, “Present and future ICT infrastructures for a smarter grid in Japan,” in *Proc. Innov. Smart Grid Technol.*, pp. 1–5, Jan. 2010.

[27] M. Newman, “The structure and function of complex networks,” *SIAM Rev.*, vol. 45, no. 2, pp. 167–256, May 2003.

[28] H. Chen, H. Jin, J. Sun, D. Deng, and X. Liao, "Analysis of large-scale topological properties for peer-to-peer networks," in *Proc. IEEE Int. Symp. Cluster Comput. Grid*, Apr. 2004, pp. 27–34.

[29] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Syst. J.*, vol. 6, no. 3, pp. 481–487, Sep. 2012.

[30] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E*, vol. 66, no. 6, Dec. 2002, Art. no. 65102.

[31] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proc. Nat. Acad. Sci.*, vol. 108, no. 10, pp. 3838–3841, Mar. 2011.

[32] Power System Cases, [Online]. Available: https://icseg.iti.illinois.edu/power-cases/, 2016.

[33] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection,"[Online]. Available: http://snap.stanford.edu/data, Jun. 2014.

[34] A. Sen, A. Mazumder, J. Banerjee, A. Das, and R. Compton, "Identification of k most vulnerable nodes in multi-layered network using a new model of interdependency," in *Proc. IEEE Conf. Comput. Commun. Workshops*, Apr. 2014, pp. 831–836.

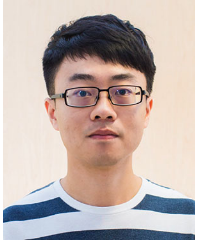
Dong Liu (Member, IEEE) received the B.Eng. (Hons) degree in electronic engineering with first class from The Hong Kong Polytechnic University, Hong Kong, in 2014, B.Eng. degree in microelectronics from Sun Yat-sen University, Guangzhou, China, in 2014, and the Ph.D. degree from Hong Kong Polytechnic University, Hong Kong, in 2019.

He was a Postdoc with the Institute of Textile and Clothing at Hong Kong Polytechnic University, and is currently a Postdoc with the Department of Electrical Engineering at City University of Hong Kong. His research interests include applications of complex networks, cyber-physical systems, machine learning for robustness assessment in smart grids.

Chi K. Tse (Fellow, IEEE) received the B.Eng. (Hons.) degree with first class honors and the Ph.D. degree from the University of Melbourne, Australia, in 1987 and 1991, respectively, both in electrical engineering.

He is currently the Chair Professor of electrical engineering with the City University of Hong Kong, Hong Kong, and was the Chair Professor and Head of electronic and information engineering with Hong Kong Polytechnic University, Hong Kong. His research interests include power electronics, nonlinear systems, and complex network applications.

Dr. Tse was the recipient of a number of research and industry awards, including Prize Paper Awards by IEEE TRANSACTIONS ON POWER ELECTRONICS in 2001, 2015 and 2017, RISP JOURNAL OF SIGNAL PROCESSING Best Paper Award in 2014, Best paper Award by *International Journal of Circuit Theory and Applications* in 2003, two Gold Medals at the International Inventions Exhibition in Geneva in 2009 and 2013, a Grand Prize and Gold Medal at the Silicon Valley International Invention Festival in 2019, and a number of recognitions by the academic and research communities, including honorary professorship by several Chinese and Australian universities, Chang Jiang Scholar Chair Professorship, IEEE Distinguished Lectureship, Distinguished Research Fellowship by the University of Calgary, Gledden Fellowship and International Distinguished Professorship-at-Large by the University of Western Australia. He serves and has served as Editor-in-Chief for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS II (2016–2019), *IEEE Circuits and Systems Magazine* (2012–2015), and *IEEE Circuits and Systems Society Newsletter* (since 2007), Associate Editor for three IEEE Journal/Transactions, Editor for *International Journal of Circuit Theory and Applications*, and is on the editorial board of the IEEE PROCEEDINGS.



Xi Zhang (Member, IEEE) received the B.Eng. degree from Beijing Jiaotong University, Beijing, China, in 2013 and the Ph.D. degree from Hong Kong Polytechnic University, Hong Kong, in 2017, both in electrical engineering.

He was a Postdoc with the Power Systems Department of China Electric Power Research Institute, Beijing, China, from 2018 to 2019. Since 2020, he has been an Assistant Professor with the School of Automation, Beijing Institute of Technology, Beijing, China. His research interests include complexity, resilience and stability analysis of the power system with high penetrations of power electronic devices.