第 2 卷 第 6 期 全球能源互联网 Vol. 2 No. 6
2019 年 11 月 Journal of Global Energy Interconnection Nov. 2019
文章编号：2096-5125 (2019) 06-0523-07 中图分类号：TM73 文献标志码：A
DOI：10.19705/j.cnki.issn2096-5125.2019.06.001

考虑信息节点失效的电力信息物理系统脆弱性评估方法

连祥龙，张文浩，钱瞳，唐文虎 *
（华南理工大学电力学院，广东省 广州市 510640）

Vulnerability Assessment of Cyber Physical Power System Considering Cyber Nodes Failure

LIAN Xianglong, ZHANG Wenhao, QIAN Tong, TANG Wenhu*
(School of Electric Power Engineering, South China University of Technology, Guangzhou 510640, Guangdong Province, China)

Abstract: As a result of deep integration of information systems and power grids, existing grid systems are developing into a form of cyber physical power system that can deal with physical damage as well as cyber attacks. This study considered threats in a power grid and formulates a fault model in which the information system and the physical layer are coupled with each other. Furthermore, an assessment index is proposed taking the importance of grid nodes and the topology of the information network into consideration. A simulation is performed in which the attacker attacks the high-index nodes and causes them to fail. The grid is optimized for minimum load reduction to identify the vulnerable links of the coupled network based on the proposed indicators. The IEEE-30 node system is used as an example. Simulation results show that the information physical network has high robustness against random attacks and high vulnerability when the high-index nodes are attacked.

Keywords: cyber physical power system; vulnerability assessment; integrated modeling

摘 要：随着信息系统与电力物理系统的深度融合，现有电网系统正在向电力信息物理系统（cyber physical power system, CPPS）发展，CPPS不仅需要应对来自物理层面的破坏，还受到来自信息层面的威胁。针对电网所受的威胁，建立了信息物理层相互耦合的故障模型，提出了一种综合电力节点重要程度及信息网络拓扑结构的评估指标。在仿真研究中，攻击者对高指标节点进行信息攻击并导致其失效，电网以负荷削减最小量为目标进行优化调度，进而根据所提指标辨识耦合网络脆弱环节。以IEEE-30节点系统作为算例进行分析，仿真结果表明，电力信息物理网络应对随机攻击时具有较高的鲁棒性，但同时高指标节点被蓄意攻击情况下则呈现较高的脆弱性。

关键词：电力信息物理系统；脆弱性评估；一体化建模

0 引言

随着智能电网建设工作的不断推进，越来越多智能传感设备投入到电网运行中，为监测电网的安全运行提供了有效的信息支持，信息网络与电力物理网络的融合达到了新的高度。传统电力系统逐渐发展成为了信息侧与物理侧高度互联互通的电力信息物理系统[1]。

深度融合的CPPS提高了电网的可观性，系统运维人员可以更好地研究、改进电网。与此同时，由于信息系统与物理系统之间的深度交互影响，也引入了新的不确定因素，给电网研究工作带来了新的挑战。如2015年乌克兰大规模停电事故的发生就是由于其西部多个区域的电网遭到了黑客的网络攻击，恶意攻击使得电力信息系统部分环节失效（控制服务器关机），从而影响物理电网的运行，造成了区域性大停电的严重后果[2]。这次大规模停电事件警示人们，在电力网与信息网络高度融合的背景下，信息系统的故障或其遭受的攻击，在危害信息系统运行的同时还会危及到电网的正常工作。由此可见，在对电力系统进行脆弱性评估时，不仅要分析电网侧故障情况，也需要结合信息网络的脆弱性，对CPPS进行综合脆弱性评估。

现有CPPS脆弱性评估研究主要集中在以下几个方面：信息网与物理网互联关系一体化建模研究、攻击方式研究、脆弱性指标研究、防护措施研究等。其研究思路可以概述为在建立一套合理的信息物理网模型的基础上，提出能够评估该模型脆弱性的指标，在特

基金项目：国家自然科学基金（基于图嵌入理论的电网弹性评估及其恢复力提升优化方法研究，51977082）；中央高校基本科研业务费专项资金资助（51477054）。

National Natural Science Foundation of China (Investigation on resilience assessment for electric power systems and optimization of its recovery capability based upon the graph embedding theory, 51977082); The Fundamental Research Funds for the Central Universities(51477054).

定攻击模式下验证该指标的有效性，最后根据模型特点提出有效的防护措施以达到降低电网脆弱性的目标。文献[3]运用加权度数、介数指标对CPPS节点重要度进行排序，并研究了相应的防护策略，对CPPS模型研究具有一定的参考价值。文献[4]采用信息节点度数和电气介数分别作为信息网络和物理网络边权，建立CPPS关联矩阵，构建节点生存率及电力负荷生存率指标进行脆弱性分析。在遭受网络攻击后，电力网络会裂解为一个主网和许多个孤岛，攻击后主网节点数与攻击前电网总节点数的比值作为连通性指标以评估电网的脆弱性[5]，该指标忽略了孤岛中发电机和负荷平衡的可能性。文献[6]提出了融合信息决策处理和物理设备动态模型的信息物理风险传递模型。文献[7]结合电力节点重要程度及信息网络拓扑情况提出了有效中心距离以评估CPPS脆弱性。文献[8] 基于相互依存网络理论，评估信息网与电力网的拓扑互相似性，研究低度数节点加边策略及其分配策略，对增强网络架构有一定的参考意义。文献[9]构建CPPS攻防博弈模型，建立了3层数学优化模型，对CPPS信息攻击下故障情况进行了分析，从攻防博弈的角度确定了双方分配攻击与防御资源量的多寡。文献[10]将智能变电站分为应用层、控制层及运行层，考虑了软件失效对CPPS运行的影响，建立了软件失效模型及信息运行设备失效模型，对实际变电站的控制与运行有一定的借鉴意义。

目前，各国对于CPPS脆弱性评估研究尚处于起步阶段，但对传统电力网络的脆弱性研究较为成熟。传统电力网络脆弱性研究主要分为基于电路机理的研究及根据复杂网络理论对电力网络进行分析。文献[11]根据电网脆性关联度及风险熵对复杂电网连锁故障薄弱环节进行识别。文献[12-13]采用电气介数、电气距离的指标从复杂网络理论的角度对电网进行脆弱性分析。当然，CPPS具有双网耦合的特性，若只从电网侧进行脆弱性分析，得到的结果不够全面，与实际情况有一定的偏差。

为了更好地分析CPPS网络实际的脆弱性，本文结合信息网络及电力网络的特点，以及其耦合关系，构建综合性评价指标，再根据指标特点采取可行性策略进行防护，降低电网脆弱性。信息节点失效后，该节点无法与外界进行通信，控制中心对其电气信息的获取及控制功能均无法正常进行。针对二次侧的本地保护，本文默认信息节点失效时继电保护装置同样遭受攻击，无法正常动作。对于保护装置仍能正常工作的情况，暂不在本文讨论范围内。本文主要工作如下：建立了信息网络与电力网络相互融合的一体化研究模型，考虑了信息节点失效对电网运行的影响，提出综合考虑电力节点重要程度和信息网络拓扑重要度的评估指标，对CPPS进行脆弱性评估，并采用IEEE-30节点系统进行了仿真验证。

1 电力–信息一体化耦合模型

随着大量新型传感设备的投入使用，CPPS能够更好地感知电网的运行情况，为电网安全可靠运行提供了支持。CPPS与传统电网最大的区别在于信息层与物理层的深度耦合，物理网为信息网络提供电力支持，信息系统将控制信号传递给电网从而起到控制作用[14]。本章将建立一个的电力-信息一体化耦合模型，以便更好地分析CPPS的脆弱性。

1.1 电力节点与信息节点耦合影响

在电力网中，其能量传输服从潮流分布，同时电力节点为其所对应的信息节点提供电力支持；不同于电力网络，信息节点之间信息包的传递总要选择最短路径，并忽略其他路径在该信息包上的作用[15]，信息节点为其所对应的电力节点提供数据采集、信息传递和控制作用。为了更好地研究CPPS脆弱性，本文对电力与信息网耦合机制进行了简化，该简化模型由物理节点、信息节点及物理-信息依存边组成。

1）物理节点N_p：每个物理节点表示发电厂、变电站等场站设施，其控制发电机出力或连接负荷。物理节点失效，该节点发电机及负荷皆切除。

2）信息节点N_c：由调度中心、信息站点等组成，信息节点采集与之相连的物理节点信息，并和其他信息节点一同组成信息网。信息节点失效，则该节点所连物理节点的发电机及负荷都无法进行切机或切负荷操作，同时与其相连的信息连接边也自动移除。

3）物理-信息依存边$E_{c\text{-}p}$：为信息节点与电力节点连接边，虚拟信息物理交互过程，此过程被简化为信息节点从物理节点采集数据、信息节点发送指令到物理节点的过程。

电力网络G_p由电力节点N_p及电力边E_p组成，信息网络G_c由信息节点N_c及信息连接边E_c组成，电力网络、信息网络及物理-信息依存边共同组成了CPPS的网络架构。

1.2 完全一一对应模型

根据上述简化方法，将CPPS简化为物理节点、信

息节点、物理−信息依存边组成的模型，电力节点的连接关系根据实际情况进行连接，信息节点之间的连接为无标度网络[15]连接方法。以上构成了信息、物理网络的单侧模型。由于CPPS双网耦合的特殊性，只建立单侧网络显然是不够的。在输电网中，控制中心需要对各母线的电压、电流、功率等电气状态进行实时监控。因此，本文在各电力节点都配置相应的信息节点，以实现控制中心通过信息网络对各电力节点的监测与遥控功能。本文运用“完全一一对应模型”来描述电力网络和信息网络相互耦合的影响，其网络结构模型如图1。

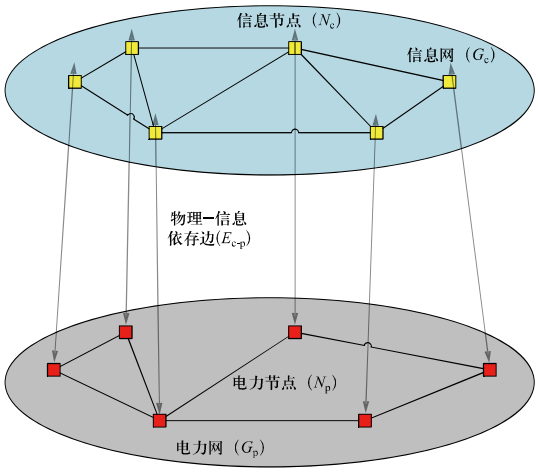

图 1　相互依存网络模型

Fig. 1　Interdependent network model

该模型中，电力节点与信息节点个数相同，且一个电力节点只与一个信息节点存在相互依存的关系。即意味着当某一个电力节点失效，该节点无法调整发电机出力及负荷量，与之相连的物理连接边及信息−物理依存边均失效；而某一信息节点失效时，无法对其相依存的电力节点进行控制，该电力节点将按照信息节点失效前时刻状态继续运行。

至此，电力网络与信息网络耦合模型已构建完成，该模型既考虑了信息网络和物理网络各自特点，又根据相互耦合关系建立了相互依存边，根据实际情况进行了适当的简化，能够在一定程度上反映CPPS故障情况。

2　CPPS脆弱性评估

2.1　电力−信息耦合故障模型

近年来，各国针对电力系统的蓄意攻击事件时有发生[16-18]，由于信息网络在电力系统中的地位不断上升，攻击者为了达到破坏电网的目的，通过物理攻击与信息攻击协同的方式，使得破坏最大化。本文从攻击者视角，攻击系统中高脆弱性节点，计算不同场景下系统损失情况，通过负荷切除量的多少来评估系统的脆弱性环节。

当电力网络发生N−1故障时，会引发电网潮流转移。此时若能够及时切除一些不重要的负荷，可以减少故障对电网稳定运行的冲击。但由于信息攻击的作用，电网的可观性和可控性均下降。为了更好地研究信息攻击对CPPS脆弱性的影响，基于直流潮流算法的高效率和收敛性强等优势，本文采用直流潮流算法对电网进行简化计算。

当电网发生N−1故障时，若信息网络正常运行，其监测、控制功能完备，控制中心可通过调控手段如控制发电机出力及负荷的切除以减小故障对电网的冲击。当信息网络遭受攻击时，其对电网的运行主要产生以下两方面的影响：①信息节点$N_{c,i}$失效，则与其依存的电力节点$N_{p,i}$所控制的发电机出力及负荷不可控，无法进行切机、切负荷操作；②若节点i与节点j所连电力边$E_{p,ij}$两端电力节点对应的信息节点均失效，则该电力边不可观，无法判断该支路潮流是否越限，不进行相应的优化操作，可能导致故障蔓延。

2.2　最优负荷削减模型

发生故障后，遍历电力网络中每一个节点，确认每个节点及连接边的工作状态，包括支路潮流分布情况及电网可观、可控情况等。当支路潮流越限时，采取切除越限最严重支路、切除发电机出力及负荷等操作。基于直流潮流模型，以削减负荷量最少为目标，其优化模型为：

$$\min f=\sum_{i=1}^{n}\Delta P_{\mathrm{F}i} \tag{1}$$

$$\text{s.t.}\quad F=A_{\mathrm{F\text{-}P}}P \tag{2}$$

$$\sum_{i=1}^{n}(P_{\mathrm{G}i}+\Delta P_{\mathrm{G}i}-(P_{\mathrm{F}i}-\Delta P_{\mathrm{F}i}))=0 \tag{3}$$

$$\left|F_l\right|\leqslant F_{l\max} \tag{4}$$

$$-P_{\mathrm{G}i}\leqslant\Delta P_{\mathrm{G}i}\leqslant P_{\mathrm{G}i\max}-P_{\mathrm{G}i} \tag{5}$$

$$0\leqslant\Delta P_{\mathrm{F}i}\leqslant P_{\mathrm{F}i} \tag{6}$$

式中：n为电力节点个数；$P_{\mathrm{G}i}$和$P_{\mathrm{F}i}$分别为电力节点i所控制的发电机出力及负荷量；$\Delta P_{\mathrm{G}i}$为电力节点i发电机出力调整量；$\Delta P_{\mathrm{F}i}$为电力节点i负荷削减量；F为支路潮流向量；$A_{\mathrm{F\text{-}P}}$为关联导纳矩阵；P为节点注入功率向

量；F_l为支路l潮流；$F_{l\max}$为支路l的潮流限值，本文取为该支路原始潮流的1.5倍。应注意的是：当某一信息节点i失效时，其对应的电力节点不可控，ΔP_{Gi}、ΔP_{Fi}均为0。

2.3 脆弱性评估指标

脆弱性评估指标是根据电网参数反映系统脆弱性情况的指标，该指标的确定是脆弱性评估中重要一环，只有选取合适的指标才能反映系统真实情况。因此，本文结合电力节点重要程度及信息拓扑重要程度，提出了权重度数及权重介数指标以评估CPPS的脆弱性。

2.3.1 权重度数

在复杂网络理论中，某节点的度数是指与该节点所连边的数目，反映了该节点在整个网络中局部重要程度，度数越大说明该节点与其余节点联系越多，但无法反映该节点在整个网络中的重要程度。在CPPS中，当信息节点失效，其所连信息边也失效，高度数节点的失效会带来更多的失效信息边，将会影响信息网络的传输性能；同时，电力节点所掌握的资源量（发电机出力与负荷量之和）用以描述电力节点的重要程度，在发生故障时，其资源量越大，则具有更多的可调控资源，通过调控这些资源，可以使电网运行在安全范围内。基于文献[3]的研究，进一步简化了权重度数指标，综合考虑电力节点所掌握资源量与信息网络节点度数，其数学表达式如下：

$$w_i = d_i / \sum d_i \tag{7}$$

$$p_i = (P_{Gi} + P_{Fi}) / (\sum P_{Gi} + \sum P_{Fi}) \tag{8}$$

$$q_i = w_i p_i \tag{9}$$

式中：d_i为信息节点i度数；w_i为信息节点度数重要度；p_i为电力节点资源重要度；q_i为权重度数。

2.3.2 权重介数

节点介数为网络中所有最短路径经过该节点的路径数目占所有最短路径总数的比值。信息网络的传输服从最短路由原则，即信息节点之间信息包的传递总要选择最短路径，并忽略其他路径在该信息包上的作用。介数是能够较好反映信息节点在信息拓扑中重要程度的指标。与度数指标不同的是，介数反映了节点在网络的全局重要度，在信息节点介数基础上，结合与其耦合电力节点资源量指标，基于文献[3]的研究，进一步简化了评价指标，提出权重介数指标：

$$v_i = \sum_{s \neq t} \delta_{st}(i) / \delta_{st} \tag{10}$$

$$u_i = v_i' \cdot p_i \tag{11}$$

式中：δ_{st}为信息节点s到t之间所有路径的数目；$\delta_{st}(i)$为信息节点s到t之间经过信息节点i的数目；v_i为信息节点i介数；v_i'为其归一化[6]结果；u_i为权重介数。

2.4 脆弱性评估流程

考虑信息节点失效下脆弱性评估流程如图2所示，主要包括以下步骤。

1）输入系统参数，建立电力网络模型、信息网络模型及相依网络模型组成的CPPS结构模型，确定系统初始状态。

2）计算权重度数、介数指标并排序，对高权重度数、介数信息节点进行信息攻击并导致其失效，确定电力元件的可观性及可控性。

3）计算支路开断后潮流，找到可观支路中越限最严重支路，若该支路越限，则切除该支路并进行切负荷及调整发电的出力优化调整。

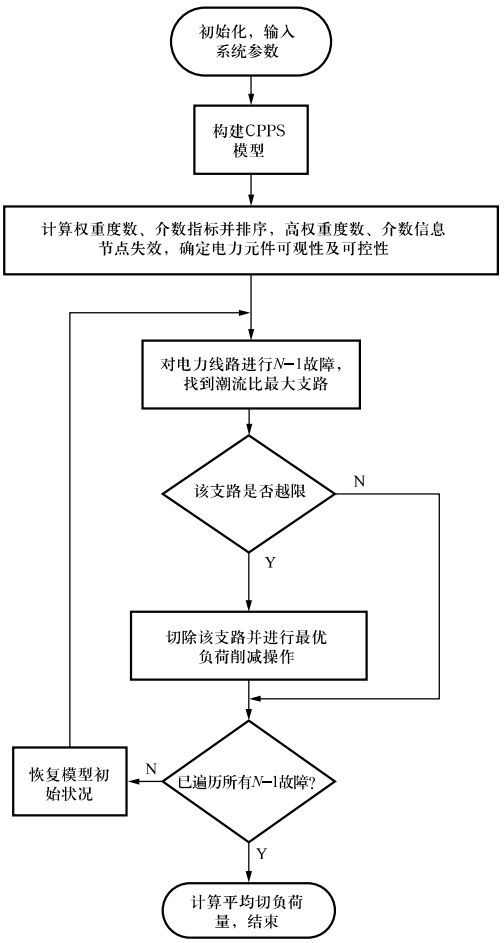

图 2 CPPS脆弱性评估流程

Fig. 2 Vulnerability assessment process of CPPS

4）根据电网实际运行状态检查支路运行情况，若都正常运行，则进行下一条支路越限故障开断，转入步骤3。

5）遍历所有$N-1$故障后，计算所有切负荷量的平均值。

3　算例与仿真结果分析

本文以IEEE-30节点系统为例进行仿真验证，仿真软件为MATLAB，文献[19]表明信息网络具有明显的无标度特性。信息网络按文献[19]方法生成2个m=1和m=2的无标度信息网，其中m为每次增加新节点的边数，m=1的无标度信息网络拓扑图如图3所示。

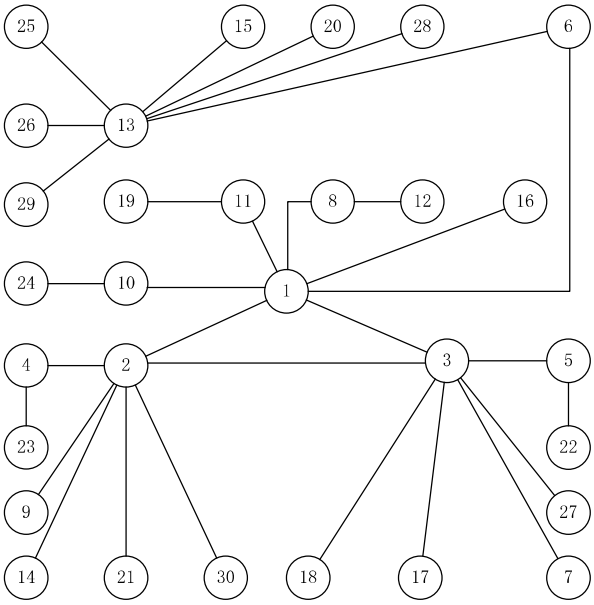

图 3　m=1时无标度信息网络拓扑

Fig. 3　Scale-free information network topology (m=1)

遍历$N-1$故障，本文仿真了面对不同信息攻击情况下，系统切除负荷量的情况。为更好地反映结果，设置排序前4的信息节点失效情况（除去节点1、2分别为平衡节点和信息中心节点，该节点重要程度极高，攻击难度大）。如高权重介数信息节点失效、m=1时，其因信息攻击失效节点为3、4、8、13节点，后续失效节点有5、7、17、18、22、27、23、12、15、20、25、26、28、29号节点。

根据以上假设，对该系统进行了仿真，并用切除负荷的平均值、最大值、不可观越限支路数来反映本次仿真结果，仿真结果如表1所示。

表 1　各种攻击模式下对系统影响情况

Table 1　Impact on the system under various attack modes

模式	切除负荷平均值/MW	切除负荷最大值/MW	不可观越限支路出现次数
不考虑信息节点失效时	6.96	36.05	0
随机节点失效模式	18.96	89.92	0
高度数节点失效（m=1）	39.39	167.75	2
高度数节点失效（m=2）	8.30	38.69	0
高介数节点失效（m=1）	20.03	147.44	6
高介数节点失效（m=2）	9.40	49.62	0
高权重度数节点失效（m=1）	25.14	138.95	4
高权重度数节点失效（m=2）	23.06	103.09	0
高权重介数节点失效（m=1）	27.79	115.06	5
高权重介数节点失效（m=2）	24.06	102.01	0

仿真结果表明，当重要信息节点失效时，电网的可靠性大大降低；当m=1时，信息网架过于简单，攻击者通过高度数、高介数攻击指标对电网进行攻击，就能使电网失去较多负荷，其可观性也大大下降；但只要通过提高信息网结构连通性（m=2）即可大大提高电网的可靠性，因此加强网架结构的建设、提高信息网络的连通性，能够大幅降低CPPS的脆弱性。

其次，在高权重度数、高权重介数攻击模式下，改进信息网络拓扑的结构对提高电网可靠性作用有限。这两种攻击模式下，系统切除了大量的负荷，其节点重要性不言而喻。因此高权重度、介数能更好地反映CPPS的脆弱性。信息物理网络应对随机攻击时具有较高的鲁棒性，同时高指标节点被蓄意攻击情况下则呈现较高的脆弱性。根据高权重度、介数指标对CPPS节点进行排序，加大对高指标节点防御措施的维护，从而可减少重要节点受到网络攻击时失效概率。

最后，当m=1时，对比权重介数指标，6号节点的重要性在度数指标中无法反映出来，从度数指标来

看，13号节点重要性比6号节点高，而仿真结果表明，当6号节点失效时，其带来的后果将比13号节点失效时严重得多。因此验证了介数指标在全局重要性上优于度数指标。

综上所述，本文所建立的电力-信息网络一体化模型能够较好地反映CPPS运行情况，所构建的权重度数、权重介数指标综合考虑了电力网络节点重要程度及信息网络拓扑情况，能较全面地反映CPPS节点重要程度。

4 结语

本文首先梳理了目前CPPS脆弱性评估研究现状，其次建立了电力信息物理网络一体化模型，提出了权重度数、权重介数指标，最后在IEEE-30节点系统中进行了仿真验证。本文研究了信息网络与电力网络耦合关系，建立了一个双网耦合模型，提出了描述CPPS脆弱性指标，确定CPPS脆弱点，对提高CPPS安全可靠运行具有指导意义。明确CPPS中的脆弱性，为提高电力系统鲁棒性提供了参考。随着电力网络与信息网络进一步融合，CPPS脆弱性评估在研究危害电力系统安全可靠运行的分析上有一定的工程应用价值。

参考文献

[1] 赵俊华，文福拴，薛禹胜，等. 电力CPS的架构及其实现技术与挑战[J]. 电力系统自动化，2010，34(16)：1-7.
Zhao Junhua, Wen Fushuan, Xue Yusheng, et al. Cyber physical power systems: architecture, implementation techniques and challenges[J]. Automation of Electric Power Systems, 2010, 34(16):1-7(in Chinese).

[2] 郭庆来，辛蜀骏，王剑辉，等. 由乌克兰停电事件看信息能源系统综合安全评估[J]. 电力系统自动化，2016，40(5)：145-147.
Guo Qinglai, Xin Shujun, Wang Jianhui, et al. Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout[J]. Automation of Electric Power Systems, 2016, 40(5):145-147(in Chinese).

[3] 张殷，肖先勇，李长松. 考虑信息物理交互的电力-信息耦合网络脆弱性分析与改善策略研究[J]. 电网技术，2018，42(10)：3136-3144.
Zhang Yin, Xiao Xianyong, Li Changsong. Vulnerability analysis and improvement strategy of power-information coupled networks considering cyber physical interaction[J]. Power System Technology, 2018, 42(10): 3136-3144 (in Chinese).

[4] 曲朝阳，董运昌，曲楠，等. 计及负荷优化重配的电力CPS可生存性量化评估[J]. 电力系统自动化，2019，43(6)：15-24.
Qu Zhaoyang, Dong Yunchang, Qu nan, et al. Quantitative survivability assessment of power cyber-physical system considering optimized load redistribution[J]. Automation of Electric Power Systems, 2019, 43(6): 15-24(in Chinese).

[5] 谭阳红，罗研彬，谭鑫，等. 电力信息物理融合系统结构脆弱性分析[J]. 湖南大学学报（自然科学版），2018，45(8)：91-98.
Tan Yanghong, Luo Yanbin, Tan Xin, et al. Analysis on structural vulnerabilities of cyber physical power systems[J]. Journal of Hunan University(Natural Sciences), 2018, 45(8): 91-98(in Chinese).

[6] 吴润泽，张保健，唐良瑞. 双网耦合模型中基于级联失效的节点重要度评估[J]. 电网技术，2015，39(4)：1053-1058.
Wu Runze, Zhang Baojian, Tang Liangrui. A cascading failure based nodal importance evaluation method applied in dual network coupling model[J]. Power System Technology, 2015, 39(4): 1053-1058(in Chinese).

[7] Saleh Soltan, Gil Zussman. EXPOSE the line failures following a cyber-physical attack on the power grid[J]. IEEE Transactions on Control of Network Systems, 2019, 6(1): 451-461.

[8] 冀星沛，王波，董朝阳，等. 电力信息-物理相互依存网络脆弱性评估及加边保护策略[J]. 电网技术，2016，40(6)：1867-1873.
Ji Xingpei, Wang Bo, Dong Zhaoyang, et al. Vulnerability evaluation and link addition protection strategy research of electrical cyber-physical interdependent networks[J]. Power System Technology, 2016, 40(6): 1867-1873(in Chinese).

[9] 石立宝，简洲. 基于动态攻防博弈的电力信息物理融合系统脆弱性评估[J]. 电力系统自动化，2016，40(17)：99-105.
Shi Libao, Jian Zhou. Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model[J]. Automation of Electric Power Systems, 2016, 40(17):99-105(in Chinese).

[10] 韩宇奇，郭嘉，郭创新，等. 考虑软件失效的信息物理融合电力系统智能变电站安全风险评估[J]. 中国电机工程学报，2016，36(6)：1500-1508.
Han Yuqi, Guo Jia, Guo Chuangxin, et al. Intelligent substation security risk assessment of cyber physical power systems incorporating software failures[J]. Proceedings of the CSEE, 2016, 36(6): 1500-1508(in Chinese).

[11] 刘文颖，王佳明，谢昶，等. 基于脆性风险熵的复杂电网连锁故障脆性源辨识模型[J]. 中国电机工程学报，2012，32(31)：142-149.
Liu Wenying, Wang Jiaming, Xie Chang, et al. Brittleness source identification model for cascading failure of complex power grid based on brittle risk entropy[J]. Proceedings of the CSEE, 2012, 32(31):142-149(in Chinese).

[12] 徐林，王秀丽，王锡凡. 电气介数及其在电力系统关键线路

识别中的应用[J]. 中国电机工程学报，2010，30(1)：33-39.
Xu Lin, Wang Xiuli, Wang Xifan. Electric betweenness and its application in vulnerable line identification in power system[J]. Proceedings of the CSEE, 2010, 30(1):33-39(in Chinese).

[13] 谭玉东，李欣然，蔡晔，等. 基于电气距离的复杂电网关键节点识别[J]. 中国电机工程学报，2014，34(1)：146-152.
Tan Yudong, Li Xinran, Cai Ye, et al. Critical node identification for complex power grid based on electrical distance[J]. Proceedings of the CSEE, 2014, 34(1): 146-152(in Chinese).

[14] 陈柯任，文福拴，赵俊华，等. 考虑物理–信息虚拟连接的电力信息物理融合系统的脆弱性评估[J]. 电力自动化设备，2017，37(12)：67-72.
Chen Keren, Wen Fushuan, Zhao Junhua, et al. Vulnerability assessment of cyber-physical power system considering virtual cyber-physical connections[J]. Electric Power Automation Equipment, 2017, 37(12): 67-72(in Chinese).

[15] 徐林，王秀丽，王锡凡. 使用等值导纳进行电力系统小世界特性识别[J]. 中国电机工程学报，2009，29(19)：20-26.
Xu Lin, Wang Xiuli, Wang Xifan. Small-world feature identification based on equivalent admittance for power system[J]. Proceedings of the CSEE, 2009, 29(19):20-26(in Chinese).

[16] 阮振，吕林，刘友波，等. 考虑负荷数据虚假注入的电力信息物理系统协同攻击模型[J]. 电力自动化设备，2019，39(2)：181-187.
Ruan Zhen, Lyu Lin, Liu Youbo, et al. Coordinated attack model of cyber-physical power system considering false load data injection[J]. Electric Power Automation Equipment, 2019, 39(2): 181-187(in Chinese).

[17] Sergey V. Buldyrev, Roni Parshani, Gerald Paul, et al. Catastrophic cascade of failures in interdependent networks[J]. Nature, 2010, 464(7291): 1025-1028.

[18] I.Dobson, B.A. Carreras, V.E.Lynch, et al. An initial model for complex dynamics in electric power system blackouts[C]// Hawaii International Conference on System Sciences, IEEE, Maui, USA, 2001.

[19] Albert-László Barabási, Reka Albert. Emergence of scaling in random networks[J]. Science, 1999, 286(5439): 509-512.

收稿日期：2019–06–30；修回日期：2019–08–07。

作者简介：


连祥龙

连祥龙（1995），男，硕士研究生，研究方向为电力信息物理系统脆弱性评估。

张文浩（1994），男，博士研究生，研究方向为微电网控制运行、信息物理融合系统。

钱瞳（1992），男，博士研究生，研究方向为分布式协调控制运行、多代理系统、微电网控制运行。

唐文虎（1974），男，教授，IEEE高级会员，IET会士，华南理工大学电力学院院长，研究方向为可再生能源发电系统建模与控制、电网设备运维智能决策、弹性电网、电力信息物理系统。通信作者，E-mail: wenhutang@scut.edu.cn。

（责任编辑　李锡）