基于攻击者视角的电力信息物理融合系统脆弱性分析

张 殷,肖先勇,李长松
(四川大学 电气信息学院,四川 成都 610065)

摘要:基于攻击者视角分析电力信息物理融合系统的脆弱性有助于决策者辨识系统脆弱环节和潜在威胁,为开展针对性防御奠定基础。结合复杂网络理论,建立了考虑信息物理交互的电力信息物理融合系统一体化模型;在直流潮流模型下,研究了信息层元件失效对物理层故障传播的影响;从攻击者角度,建立了 4 种攻击模式,从物理层和信息层结构与功能属性出发,建立了更为全面的融合系统脆弱性指标,并对 2 种信息网拓扑结构下融合系统的脆弱性进行了分析。仿真结果表明,物理层负载水平和信息层拓扑结构是影响融合系统脆弱性的重要因素;相比随机攻击,蓄意攻击下融合系统更脆弱,协同攻击下尤为脆弱;高加权介数和高加权度数信息节点对维持信息层功能起关键作用;信息物理协同破坏效应严重恶化了系统的性能。

关键词:电力信息物理融合系统;信息物理交互;复杂网络理论;脆弱性;攻击者视角
中图分类号:TM 711 **文献标识码**:A DOI:10.16081/j.issn.1006-6047.2018.10.013

0 引言

智能电网发展背景下,现代电力系统正演化为电力信息物理融合系统,其中信息系统与物理系统深度融合,可更精确、高效地监控物理系统,但也带来新的脆弱性问题[1-2]。美加大停电[3]和意大利大停电[4]事故分析显示信息系统故障是诱发大停电的重要原因,由网络攻击引发的乌克兰大停电[5]迫使人们重视信息物理融合系统的安全问题。因此,建立电力信息物理融合系统一体化模型,研究信息层元件失效对物理层故障传播的影响,分析电力信息物理融合系统的脆弱性,对识别和保护融合系统的脆弱环节具有重要的意义。

随着信息化水平的提升,信息层和物理层的交互日益频繁,物理层对信息层的高度依赖性可能带来的问题已引起学者关注。文献[6]研究了信息安全风险在电力信息物理融合系统中的跨空间传播机制。信息层故障影响系统可观性和可控性,文献[7]研究了广域测量系统(WAMS)故障对最优负荷减载模型的影响。文献[8]提出了评估通信中断对电网实时负荷控制影响的量化方法。文献[9]建立电力网和信息网的交互模型,研究了不同路由策略和耦合方式对电网连锁故障的影响。

传统电力系统脆弱性分析方法对信息系统的影响考虑不足。为此,考虑通信故障影响,文献[10]提出了电力系统综合脆弱性评估方法。除故障外,系统还面临蓄意攻击的威胁。文献[11]研究了网络攻击引发的信息物理安全问题,将传统脆弱性分析扩展为信息物理脆弱性分析。考虑攻防双方的交互博弈,文献[12]建立攻防博弈模型,研究了电力信息物理融合系统的脆弱性。拓扑属性是复杂系统最直观的属性,复杂网络理论为电力信息物理融合系统的建模和脆弱性分析提供了新思路[13]。文献[14]将电力信息物理融合系统抽象为由电力网和信息网构成的耦合网络,基于渗流理论分析了耦合网络的脆弱性。考虑潮流特性和网络拓扑,文献[15-16]分析了电力信息物理融合系统面对随机和蓄意攻击的脆弱性,指出信息层拓扑关键节点遭受攻击对系统性能的影响明显。

攻击者可基于对系统信息的不同掌握程度制定不同攻击策略[17],而伊朗核电站事故、乌克兰大停电事件表明具有背景知识的有组织攻击者可对攻击目标实施选择性的精确攻击,甚至协同攻击[18]。因此,在统一研究框架下,基于攻击者视角建立不同攻击模式,分析电力信息物理融合系统的脆弱性,有助于揭示系统脆弱环节、潜在威胁。从网络拓扑角度,结构关键节点为高价值攻击目标[13,19],但耦合特性影响节点重要性[20],需综合考虑网络拓扑、信息物理耦合特性辨识系统的脆弱环节。文献[12]分析电力网、信息网同时受攻击的场景,但未考虑多信息节点组合攻击和攻击问题的多目标属性。此外,基于复杂网络理论的脆弱性指标多为拓扑指标,还需综合考虑信息层、物理层的结构及功能属性建立脆弱性指标。

本文首先基于复杂网络理论,构建电力信息物理融合系统一体化模型。考虑物理层的潮流特性和信息层的调度功能,研究信息层节点失效对物理层故障传播的影响,分析融合系统的脆弱性。然后,从攻击者角度,依据不同信息建立多种攻击模式,其中,在蓄意攻击中,综合网络结构和耦合特性提出加权介数和加权度数指标辨识系统的脆弱环节;在协同攻击中,考虑攻击者期望以最小代价实现攻击效果最大化的多目标属性,计及攻防交互建立攻防双层模型,揭示信息物理协同破坏效应对系统的潜在威胁。最后,综合物理层和信息层的结构与功能属

收稿日期:2017-05-13;**修回日期**:2018-04-23

性构建更为全面的融合系统脆弱性指标,分析2种信息网拓扑结构下融合系统的脆弱性。

1 电力信息物理融合系统一体化建模

电力信息物理融合系统是典型的复杂网络系统,本文基于复杂网络理论构建融合系统的一体化模型。

1.1 融合系统网络模型

从复杂网络视角,电力信息物理融合系统可抽象为由物理电网和信息网耦合而成的二元网络,包括物理层、信息层和交互层。物理层对应物理电网,将发电机、变电站等抽象为电力节点,输电线路抽象为电力边。信息层对应信息网,将调度中心、信息设备等抽象为信息节点,通信线路抽象为信息边。交互层对应信息物理交互关系,厂站信息节点与电力节点相互耦合,将网间映射关系抽象为耦合边。

结合融合系统网络模型可构造耦合网络邻接矩阵$\boldsymbol{A}$[10],其由物理电网邻接子矩阵$\boldsymbol{A}_{\mathrm{p}}$、信息网邻接子矩阵$\boldsymbol{A}_{\mathrm{c}}$、物理电网-信息网耦合子矩阵$\boldsymbol{A}_{\mathrm{p\text{-}c}}$组成,如式(1)所示。

$$\boldsymbol{A}=\begin{bmatrix}\boldsymbol{A}_{\mathrm{p}} & \boldsymbol{A}_{\mathrm{p\text{-}c}}\\ \boldsymbol{A}_{\mathrm{p\text{-}c}}^{\mathrm{T}} & \boldsymbol{A}_{\mathrm{c}}\end{bmatrix} \tag{1}$$

其中,$\boldsymbol{A}_{\mathrm{p}}$中的元素$a_{\mathrm{p},ij}$表示电力节点$V_{\mathrm{p}i}$和$V_{\mathrm{p}j}$的邻接关系,节点邻接则$a_{\mathrm{p},ij}=1$,反之则$a_{\mathrm{p},ij}=0$;$\boldsymbol{A}_{\mathrm{c}}$中的元素$a_{\mathrm{c},ij}$表示信息节点$V_{\mathrm{c}i}$和$V_{\mathrm{c}j}$的邻接关系,节点邻接则$a_{\mathrm{c},ij}=1$,反之则$a_{\mathrm{c},ij}=0$;$\boldsymbol{A}_{\mathrm{p\text{-}c}}$中的元素$a_{\mathrm{p\text{-}c},ij}$表示$V_{\mathrm{p}i}$和$V_{\mathrm{c}j}$的耦合关系,节点耦合则$a_{\mathrm{p\text{-}c},ij}=1$,反之则$a_{\mathrm{p\text{-}c},ij}=0$。

1.2 耦合网络扩展建模

1.1节从纯拓扑角度对融合系统进行网络建模,而融合系统建模还需考虑系统功能及信息物理交互。文献[14]假设的信息物理交互机制并不合理,由于不间断电源的应用,电力元件失效一般不会影响对应信息元件的正常工作[9];而信息元件失效会造成监控功能受损,但不一定会导致电力元件失效。

实际中,物理层完成电力供应,信息层对物理层进行监视与控制。其中,信息节点采集物理电网的运行状态信息,上传调度中心分析处理,若调度中心察觉物理电网运行越限,则生成调控指令下发信息节点执行,物理电网调整进入新运行状态。电力信息物理融合系统简化示意图如图1所示。

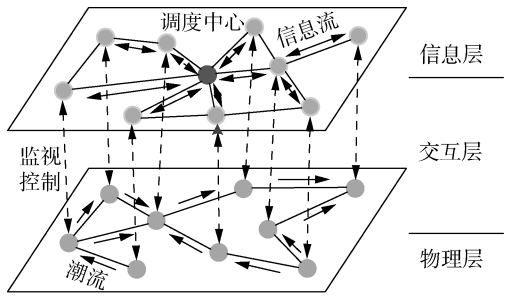

图1 电力信息物理融合系统简化示意图

Fig.1 Simplified schematic diagram of cyber physical power system

2 电力信息物理融合系统元件失效模拟

信息节点是网间交互作用点、监控功能载体,因此,本文模拟信息节点失效,研究信息节点失效对物理电网故障传播的影响,分析融合系统的脆弱性。而系统脆弱性用于描述系统在遭受攻击或设备发生故障时的性能下降情况,因此,本文基于攻击者视角,模拟4种攻击模式,深入分析融合系统的脆弱性。

2.1 元件失效模拟

传统电力系统的静态安全分析仅关注物理电网的故障,并默认信息层正常工作,必要时采取调整控制措施使电网恢复正常运行。一般过程为:电力支路开断,引发潮流重新分配,造成部分支路过载,调度中心感知到支路过载,启动优化调度消除支路过载,电网恢复正常运行。但信息节点失效将影响物理电网的可观、可控性以及故障传播。因此,有必要模拟信息节点失效的影响,分析融合系统的脆弱性。

下文将结合网络结构和系统功能模拟信息节点失效的影响。首先分析信息节点失效对网内连接的影响。若信息节点失效,则将$\boldsymbol{A}_{\mathrm{c}}$中该节点所在行、列元素修正为0,分析信息网的连通情况。引入信息节点连通因子$d_{\mathrm{c}i}$,依据修正后的$\boldsymbol{A}_{\mathrm{c}}$分析信息节点$V_{\mathrm{c}i}$与调度中心$V_{\mathrm{c}1}$的连通情况。若$V_{\mathrm{c}i}$与$V_{\mathrm{c}1}$失联,则$d_{\mathrm{c}i}=0$,节点$V_{\mathrm{c}i}$失效,修正$\boldsymbol{A}_{\mathrm{c}}$;反之,$d_{\mathrm{c}i}=1$。$d_{\mathrm{c}1}$对应调度中心,$d_{\mathrm{c}1}=d_{\mathrm{c}2}\vee d_{\mathrm{c}3}\vee\cdots\vee d_{\mathrm{c}N_{\mathrm{c}}}$,其中$\vee$表示逻辑或运算,$N_{\mathrm{c}}$为信息节点数。

信息节点失效还将影响网间耦合情况。若信息节点失效,则将$\boldsymbol{A}_{\mathrm{p\text{-}c}}$中失效信息节点所在列元素修正为0,分析电力节点耦合情况。引入电力节点耦合因子$d_{\mathrm{p}i}$,依据修正后的$\boldsymbol{A}_{\mathrm{p\text{-}c}}$分析电力节点$V_{\mathrm{p}i}$和信息节点的耦合情况,因调度中心不与电力节点耦合,则有$d_{\mathrm{p}i}=a_{\mathrm{p\text{-}c},i2}\vee a_{\mathrm{p\text{-}c},i3}\vee\cdots\vee a_{\mathrm{p\text{-}c},iN_{\mathrm{c}}}$。若当前无在运信息节点与$V_{\mathrm{p}i}$耦合,则$d_{\mathrm{p}i}=0$,电力节点$V_{\mathrm{p}i}$不可观、不可控;反之,$d_{\mathrm{p}i}=1$。

信息节点失效将导致调度中心失去对电力元件的监视与控制,影响物理电网的态势感知和优化调整[7-8,16]。对于电力边$E_{\mathrm{p},ij}$,若$d_{\mathrm{p}i}$和$d_{\mathrm{p}j}$均为0,则认为支路不可观;反之,支路可观。当可观支路潮流越限时,启动潮流优化调整;否则,不启动调整,模拟信息节点失效对电网可观性的影响。对于电力节点$V_{\mathrm{p}i}$,若$d_{\mathrm{p}i}=0$,则节点不可控;反之,节点可控。若节点可控,则对应发电机和负荷参与潮流优化调整;反之,发电机和负荷不参与调整,调整量为0,模拟信息节点失效对电网可控性的影响。本文以直流最优

潮流模拟优化调整过程,简化如下:

$$\min \sum_{i=1}^{N_p} \Delta P_{Di} \tag{2}$$

$$\text{s.t. } \boldsymbol{F} = \boldsymbol{A}_{F-P}\boldsymbol{P} \tag{3}$$

$$\sum_{i=1}^{N_p} (P_{Gi} + \Delta P_{Gi} - P_{Di} + \Delta P_{Di}) = 0 \tag{4}$$

$$-d_{pi}P_{Gi} \leqslant \Delta P_{Gi} \leqslant d_{pi}(P_{Gi\max} - P_{Gi}) \tag{5}$$

$$0 \leqslant \Delta P_{Di} \leqslant d_{pi}P_{Di} \tag{6}$$

$$-F_{l\max} \leqslant F_l \leqslant F_{l\max} \tag{7}$$

其中,N_p 为电力节点数;$\boldsymbol{F}$ 为支路潮流向量;$\boldsymbol{A}_{F-P}$ 为支路-节点关联导纳矩阵;$\boldsymbol{P}$ 为节点注入功率向量;P_{Gi} 和 ΔP_{Gi} 分别为节点 i 的发电机有功出力和调整量;$P_{Gi\max}$ 为节点 i 的发电机有功出力上限;P_{Di} 和 ΔP_{Di} 分别为节点 i 的有功负荷和削减量;F_l 和 $F_{l\max}$ 分别为支路 l 的潮流和潮流限值,$F_{l\max}$ 设为支路初始潮流的 u 倍,u 为支路传输容量系数。

2.2　基于攻击者视角的攻击模式分析

本文分析融合系统在电力支路 $N-1$ 故障下面对不同攻击模式的脆弱性,揭示严重恶化融合系统性能的脆弱环节及潜在威胁。攻击者通常会结合掌握的信息制定攻击策略,因此,从攻击者角度,依据不同攻击信息构造攻击模式。其中,不考虑对调度中心的攻击。

2.2.1　基于零信息的随机攻击模式

基于零信息的随机攻击模式为每次随机攻击一个信息节点,并逐渐增加被攻击节点的个数。

2.2.2　基于拓扑信息的攻击模式

基于拓扑信息的攻击模式为将信息节点按介数或度数从大到小排列,按顺序增加被攻击节点个数。以“介数、度数攻击”表示“基于拓扑信息的攻击”。

2.2.3　基于拓扑和耦合信息的攻击模式

信息物理耦合特性影响信息节点的重要性,本文综合考虑网络结构和耦合特性,建立加权介数和加权度数指标,构建基于拓扑和耦合信息的攻击模式。电力节点可供监控的资源量不同,因此,实现对其监控的重要度不同,影响信息节点的重要性。由此,本文从物理层角度量化监控资源,采用映射加权方法辨识重要信息节点。信息网监视电力支路的潮流情况,模拟电网态势感知。电力节点 V_{pi} 可供监视的资源量 w_{mi} 为:

$$w_{mi} = M_i \tag{8}$$

其中,M_i 为与电力节点 V_{pi} 相连的电力支路数。

信息网控制电力节点的发电机出力调整量和负荷削减量,以最优潮流模拟优化调整。若控制功能正常,由式(5)、(6)知 ΔP_{Gi} 在区间 $[-P_{Gi}, P_{Gi\max}-P_{Gi}]$ 内调整,ΔP_{Di} 在区间 $[0, P_{Di}]$ 内调整,从优化问题解空间角度,以资源调整范围区间长度量化控制资源。电力节点 V_{pi} 可供控制的资源量 w_{ci} 为:

$$w_{ci} = P_{Gi\max} + P_{Di} \tag{9}$$

资源量化值可反映对电力节点监控的重要程度,其中高资源电力节点失去监控对系统的影响大。

a. 加权介数。

介数指标从节点对网络路由的贡献角度评估节点的全局结构影响力。信息节点在物理电网监控信息传输中起路由作用,当应用介数指标评估信息节点的全局重要性时还需考虑信息网的垂直传输特性、信息物理耦合特性。在电力信息网的垂直传输特性下,调度中心仅为传输路由的起点或终点。此外,监视和控制功能属性对信息节点重要性的影响不可忽视,承担高资源电力节点信息传输的信息节点有重要作用。因此,在介数指标基础上,计及信息网的垂直传输特性,并以监控资源归一化值作为重要度指标进行映射加权,定义信息节点加权介数 B_i 为:

$$B_i = \sum_{s=V_{c1}, j\in V_p} w'_{mj} w'_{cj} \frac{\sigma_{sj}^i}{\sigma_{sj}} \tag{10}$$

其中,V_{c1} 为调度中心;V_p 为电力节点集合;w'_{mj} 为归一化处理后的监视资源 w_{mj} 的归一化值;w'_{cj} 为控制资源 w_{cj} 的归一化值;σ_{sj}、σ_{sj}^i 分别为扩展信息网中 V_{c1} 与 V_{pj} 间最短路径数目、经过信息节点 V_{ci} 的次数,可由 $\boldsymbol{A}_{ce}$ 计算获得,$\boldsymbol{A}_{ce}$ 为扩展信息网邻接矩阵,见式(11)。

$$\boldsymbol{A}_{ce} = \begin{bmatrix} 0 & \boldsymbol{A}_{p-c} \\ \boldsymbol{A}_{p-c}^T & \boldsymbol{A}_c \end{bmatrix} \tag{11}$$

扩展邻接矩阵 $\boldsymbol{A}_{ce}$ 由 $\boldsymbol{A}_c$、$\boldsymbol{A}_{p-c}$ 构成,反映信息网内邻接关系、信息物理网间耦合关系。由此,加权介数反映了信息节点对电力节点监控信息路由的贡献,同时考虑了监控功能属性对节点重要性的影响。

b. 加权度数。

度数指标可度量节点在网络中的局域结构重要性,但未考虑网间耦合特性。信息节点实现对与之耦合电力节点的信息采集与指令执行。综合考虑节点的局域结构、功能贡献度,定义加权度数指标。以节点度数度量节点局域结构贡献度,以耦合监控资源度量节点局域功能贡献度,则信息节点加权度数 D_i 为:

$$D_i = D_i^s D_i^f \tag{12}$$

其中,信息节点局域结构贡献度 D_i^s 为信息节点度数的归一化值;局域功能贡献度 D_i^f 为与信息节点耦合的监视资源和控制资源归一化值之积。

基于拓扑和耦合信息的攻击模式将信息节点按加权介数或加权度数从大到小排列,按顺序增加被攻击节点的个数。以“加权介数、加权度数攻击”表

示“基于拓扑和耦合信息的攻击”。

2.2.4 基于完全信息的攻击模式

完全信息状态下,攻击者掌握防御者(系统调度)的调控策略,经推演分析后制定优化攻击策略[12,21]。攻防双方存在交互行为,攻击者期望以最小的攻击成本实现电网损失最大化,而防御者采取调控措施以期电网损失最小化,由此,攻防过程可构建为双层模型。简化起见,假设各信息节点的攻击成本相同,以攻击节点数代表攻击成本进行研究。上层模型中,攻击者结合物理电网失效元件,配合攻击信息节点,以期借助信息物理元件失效的协同破坏效应放大电力元件失效的影响,从而攻击尽可能少的信息节点使物理层的损失尽可能大;下层模型中,防御者感知物理层的运行状态,采取调整发电机出力、切负荷等措施消除支路潮流越限,以期抑制物理层故障蔓延使物理层的损失尽可能小。

特别地,攻击者期望以最小代价实现攻击效果最大化,攻击问题具有多目标属性。由于上述问题的复杂性,常规优化算法难以求解,智能算法为近似求解此类问题提供了可能。由此,本文选取广泛应用的带精英策略的非支配排序遗传算法(NSGA-Ⅱ)[22]进行求解,求解过程如下:设定物理电网失效元件,上层模型生成包含各信息节点受攻击状态的攻击向量,传至下层模型按元件失效分析流程计算对应攻击向量下的物理层负荷损失;然后将物理层负荷损失传回上层模型,以攻击信息节点数及物理层负荷损失为适应度,经进化和筛选操作生成新的攻击向量,继续传至下层模型迭代寻优,直至达到最大迭代次数,得到攻击策略的 Pareto 最优解集,构建不同元件攻击数目下的协同攻击策略。以“协同攻击”表示“基于完全信息的攻击”。

3 电力信息物理融合系统脆弱性分析

本文从物理层和信息层的结构及功能角度综合度量融合系统的性能,提出电力信息物理融合系统脆弱性指标。

3.1 融合系统脆弱性指标

3.1.1 物理层脆弱性指标

物理层的主要功能是完成电力供应,而物理电网是实现物理层功能的基础。因此,以物理电网的结构完整度和失负荷量衡量元件失效对物理层的影响,分别如式(13)、式(14)所示。

$$D_{\mathrm{pn}}=N'_{\mathrm{p}}/N_{\mathrm{p}} \tag{13}$$

$$D_{\mathrm{pd}}=L_{\mathrm{D}}/\sum_{i=1}^{N_{\mathrm{p}}}P_{\mathrm{D}i} \tag{14}$$

其中,N'_{p}为故障后物理电网损失节点数;L_{D}为故障后物理电网损失负荷量。

3.1.2 信息层脆弱性指标

信息层为物理层提供监视与控制功能,信息网是实现信息层功能的基础。结合信息节点连通因子d_{ci},定义信息层连通脆弱性指标D_{cn}如下:

$$D_{\mathrm{cn}}=1-\frac{1}{N_{\mathrm{c}}}\sum_{i=1}^{N_{\mathrm{c}}}d_{ci} \tag{15}$$

结合耦合因子$d_{\mathrm{p}i}$、监视资源$w_{\mathrm{m}i}$和控制资源w_{ci},定义信息层监视功能脆弱性指标D_{cm}和控制功能脆弱性指标D_{cc},分别如式(16)、式(17)所示。

$$D_{\mathrm{cm}}=1-\sum_{i=1}^{N_{\mathrm{p}}}(d_{\mathrm{p}i}w_{\mathrm{m}i})/\sum_{i=1}^{N_{\mathrm{p}}}w_{\mathrm{m}i} \tag{16}$$

$$D_{\mathrm{cc}}=1-\sum_{i=1}^{N_{\mathrm{p}}}(d_{\mathrm{p}i}w_{ci})/\sum_{i=1}^{N_{\mathrm{p}}}w_{ci} \tag{17}$$

3.2 分析流程

a. 设置物理电网和信息网的初始失效元件。

b. 分析信息节点失效后的网络连通情况,更新耦合网络邻接矩阵$\boldsymbol{A}$,计算d_{ci}和$d_{\mathrm{p}i}$,确定信息节点在运状态和电力元件的可观、可控性。

c. 计算电力支路开断后物理电网潮流,若可观测支路存在越限情况,则转至步骤 **d**;若可观测支路不存在越限情况,则转至步骤 **e**。

d. 考虑电力节点的可控性,结合式(2)—(7)计算最优潮流,若收敛,则依据优化结果制定控制指令进行相应调整;若不收敛,则由于调整手段与资源不足导致无法消除支路潮流越限,不进行调整。

e. 检查物理电网支路潮流越限,若存在越限,则断开越限支路,转至步骤 **c**;若不存在越限,则故障终止,转至步骤 **f**。

f. 计算脆弱性指标,至此单次仿真结束。

4 算例分析

电力调度数据网可分为双星形和网状 2 种结构,其中,双星形网是典型的无标度网络,网状网是典型的小世界网络[23]。由此,以 IEEE 57 节点系统为例构造电力信息物理融合系统的物理层,信息层分别依据文献[24]、文献[25]中的方法生成无标度和小世界信息网。2 种网络均选择度数最大的节点为调度中心,其他节点为厂站信息节点,厂站信息节点与电力节点一对一耦合。不失一般性,分别生成 10 个无标度和小世界信息网建立耦合网络模型,统计平均脆弱性指标。

4.1 不同负载水平下的融合系统脆弱性分析

负载水平是影响电网故障传播的关键因素,本文对比分析 u 为 1.5、2 时融合系统面对随机攻击的脆弱性。设置 f 个初始失效信息节点,遍历分析电力支路 N-1 故障,统计融合系统中物理层和信息层的平均脆弱性指标D_{p}和D_{c},重复 10 次随机攻击得

到无标度和小世界信息网对应结果,如图 2、3 所示。

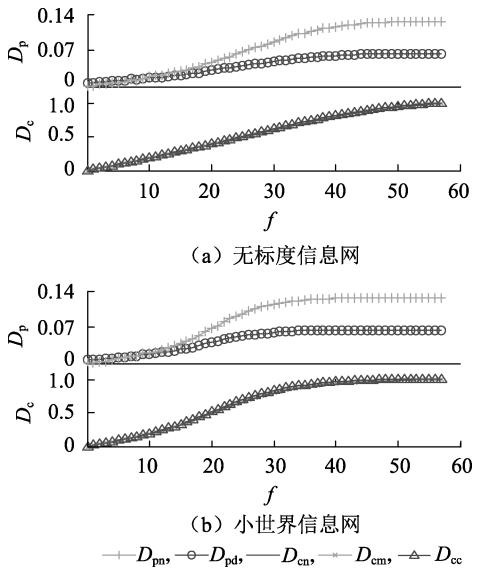

图 2　$u=2$ 时融合系统面对随机攻击的脆弱性指标

Fig.2　Vulnerability indices of cyber physical power system under random attack when $u=2$

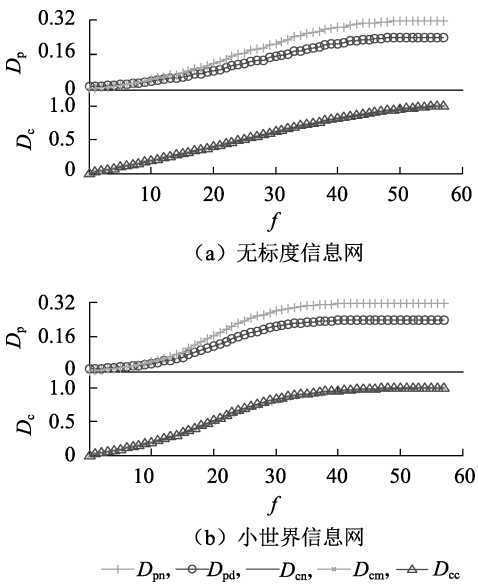

图 3　$u=1.5$ 时融合系统面对随机攻击的脆弱性指标

Fig.3　Vulnerability indices of cyber physical power system under random attack when $u=1.5$

观察图 2 可知,不同信息网拓扑结构下的融合系统的脆弱性曲线呈现相似变化趋势。当信息网无失效元件时,信息层的监控功能健全,可有效地抑制物理层故障蔓延。随着失效节点数目增加,信息网的连通性水平下降,监控功能受损加重,抑制物理层故障传播的能力下降,脆弱性指标上升。当信息网崩溃时,调度中心的监控功能完全丧失,电网潮流服从自然分布,脆弱性指标稳定。相比小世界网络,无标度网络面对随机攻击时呈现较高的鲁棒性,融合系统脆弱性曲线上升更平缓。

对比图 2、3 可知,$u=1.5$ 时,物理层的脆弱性指标曲线斜率更大、上升速度更快,表明重负载水平下信息层节点失效对物理层故障传播的影响更显著,物理层负载水平是影响融合系统脆弱性的重要因素。

4.2　不同蓄意攻击模式下的融合系统脆弱性分析

以 $u=1.5$ 为例,分析融合系统在蓄意攻击下的脆弱性。除协同攻击外,其他蓄意攻击模式均未考虑信息物理元件失效的协同配合。基于此,将蓄意攻击分为 2 类,分析不同蓄意攻击模式下融合系统的脆弱性。

4.2.1　未考虑信息物理元件失效协同配合的蓄意攻击

介数攻击、度数攻击、加权介数攻击、加权度数攻击模式均未考虑与具体物理层故障的协同配合,其攻击思路为:攻击信息层的关键节点,破坏信息层结构与功能,助推物理层的故障蔓延,恶化系统性能。仿真得到上述攻击模式下的脆弱性结果,见图 4—7。

观察图 4、5 可知,相比随机攻击,介数、度数攻击的效果更好。当信息网为无标度网络时,由于网络的无标度特性,少数拓扑关键节点的移除导致信息网的连通性水平快速下降,脆弱性曲线上升较快。当信息网为小世界网络时,由于小世界网络节点度分布较窄,且度数分布较均匀[25],度数攻击与随机攻击的攻击效果相差不大,而介数攻击的效果好。但拓扑关键节点不一定是功能关键节点,因此,对于信息层功能而言,基于拓扑信息的攻击模式属于无差别攻击。完整信息网是信息层功能实现的基础,信息层结构受损伴随功能受损,信息层脆弱性曲线大致重合,变化趋势基本一致。

观察图 6、7 可知,相比介数、度数攻击,加权介数、加权度数攻击的攻击效果更加明显。物理层脆

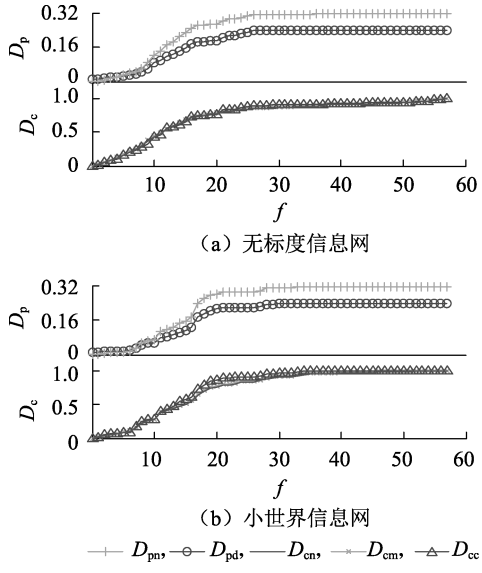

图 4　介数攻击下融合系统脆弱性指标

Fig.4　Vulnerability indices of cyber physical power system under betweenness based attack

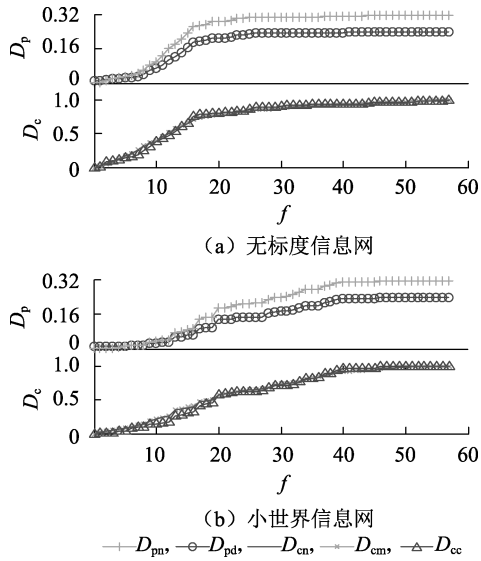

图5 度数攻击下融合系统脆弱性指标

Fig.5 Vulnerability indices of cyber physical power system under degree based attack

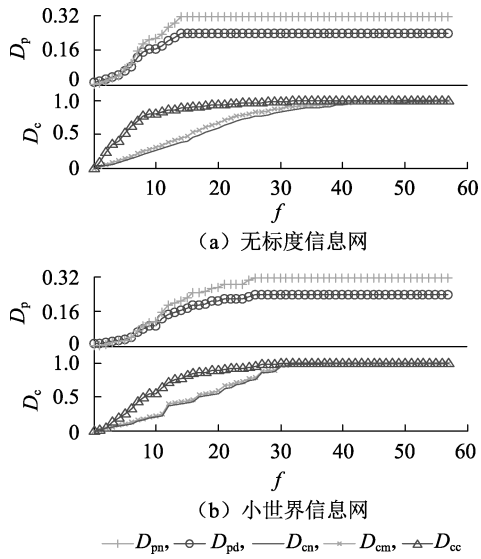

图6 加权介数攻击下融合系统脆弱性指标

Fig.6 Vulnerability indices of cyber physical power system under weighted betweenness based attack

弱性曲线斜率大、上升速度快,且信息层的脆弱性曲线不再重合。由于信息层节点对应的物理层耦合资源分布不均匀,不同信息节点对于维持信息层功能的作用不同,而加权介数和加权度数指标采用物理层资源映射加权方法,同时考虑了信息网结构特性和信息物理耦合特性对节点重要性的影响。因此,高加权介数和高加权度数信息节点为维持信息层功能的重要节点,考虑耦合特性的攻击模式实现了差异化攻击,信息层功能受损严重,物理电网的故障蔓延。总体而言,无标度信息网下融合系统面对蓄意攻击呈现较高的脆弱性,信息层拓扑结构是影响融合系统脆弱性的重要因素。

结合物理层失负荷情况从攻击效益和攻击效率

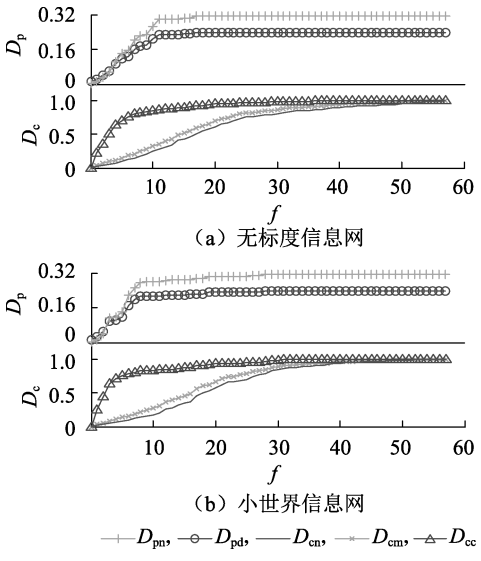

图7 加权度数攻击下融合系统脆弱性指标

Fig.7 Vulnerability indicesof cyber physical power system under weighted degree based attack

角度进一步对比不同攻击模式的攻击效果。假设各节点的攻击成本相同,以攻击节点数占比度量攻击投入,以物理层失负荷率度量攻击效益,以攻击效益最大和攻击费效比最小时的攻击参数对比展示不同攻击模式的效果,分别见表1、表2(表2中以物理层失负荷率度量攻击效益)。其中,攻击费效比为攻击投入和攻击效益的比值,数值小则攻击效率高。

表1 不同攻击模式下攻击效益最大时的攻击阈值

Table 1 Threshold values of different attack modes with maximum attack benefits

信息网	攻击模式	攻击节点数阈值	占比/%
无标度网络	介数攻击	38	66.67
	度数攻击	45	78.95
	加权介数攻击	14	24.56
	加权度数攻击	17	29.82
小世界网络	介数攻击	33	57.89
	度数攻击	46	80.70
	加权介数攻击	26	45.61
	加权度数攻击	28	49.12

表2 不同攻击模式下攻击费效比最小时的攻击参数

Table 2 Attack indices of different attack modes with minimum cost-effectiveness ratio

信息网	攻击模式	节点数	攻击效益	费效比
无标度网络	介数攻击	17	0.185 0	1.61
	度数攻击	16	0.186 9	1.50
	加权介数攻击	8	0.148 1	0.95
	加权度数攻击	5	0.116 5	0.75
小世界网络	介数攻击	19	0.205 3	1.62
	度数攻击	20	0.135 5	2.59
	加权介数攻击	12	0.147 9	1.42
	加权度数攻击	6	0.170 4	0.62

综合图4—7及表1、2可知,相比介数、度数攻击,加权介数、加权度数攻击的效果均更好。由于加权介数、加权度数综合考虑了网络拓扑和信息物理

耦合特性,高加权介数、高加权度数的信息节点为关键节点,对维持信息层的调度功能具有重要的作用。

4.2.2　考虑信息物理元件失效协同配合的协同攻击

协同攻击实现信息物理元件失效的协同配合,可借助物理层对信息层的依赖性放大电力元件失效对物理层的影响,实现攻击效果的最大化。本文以电力线路 3-4 失效为例,对比融合系统在该线路失效下不同信息节点攻击模式的物理层失负荷情况,以突出协同攻击效果、展现协同攻击的优势,如图 8 所示。其中,NSGA-Ⅱ算法种群规模为 100,最大进化代数为 50,变异因子取 0.2,交叉因子取 0.8。

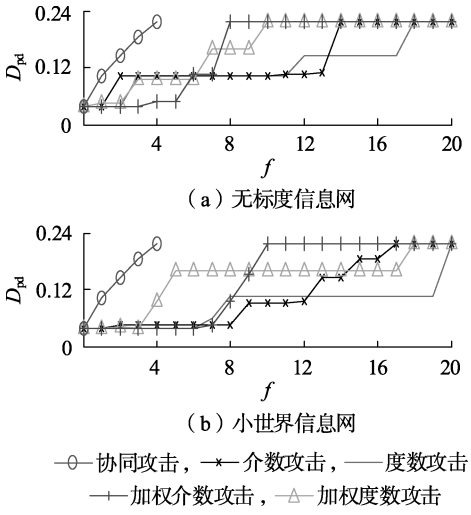

图 8　协同攻击与其他攻击模式的攻击效果对比

Fig.8　Comparison of attack effects between coordinated attack and other attack modes

观察图 8 可知,相比其他攻击模式,融合系统在协同攻击下尤为脆弱。由于协同攻击计及了信息物理协同破坏效应,仅需配合攻击少量信息元件即可严重恶化系统性能。此外,结果表明攻击者对系统信息掌握的程度越高,攻击模式越有效,也反映了强化系统信息保密对降低融合系统攻击脆弱性的意义。

5　结论

本文基于复杂网络理论建立电力信息物理融合系统的一体化模型。考虑物理层潮流特性和信息层调度功能,研究信息层节点失效对物理层故障传播的影响。从攻击者角度,依据不同攻击信息建立攻击模式,分析 2 种信息网拓扑结构下融合系统的脆弱性。仿真结果表明,物理层的负载水平、信息层的拓扑结构是影响融合系统脆弱性的重要因素。相比随机攻击,蓄意攻击下融合系统更脆弱,协同攻击下尤为脆弱,反映了强化系统信息保密对降低融合系统攻击脆弱性的意义;高加权介数、高加权度数的信息节点对维持信息层功能起关键作用,需重点保护;信息物理协同破坏效应严重恶化了系统的性能。

本文研究了融合系统面对不同攻击模式的脆弱性,下一步需结合不同攻击特点设计优化防御策略。

参考文献:

[1] 赵俊华,文福拴,薛禹胜,等. 电力信息物理融合系统的建模分析与控制研究框架[J]. 电力系统自动化,2011,35(16):1-8.
ZHAO Junhua,WEN Fushuan,XUE Yusheng,et al. Modeling analysis and control research framework of cyber physical power systems [J]. Automation of Electric Power Systems,2011,35(16):1-8.

[2] 张勇军,陈泽兴,蔡泽祥,等. 新一代信息能源系统:能源互联网[J]. 电力自动化设备,2016,36(9):1-7.
ZHANG Yongjun, CHEN Zexing, CAI Zexiang, et al. New generation of cyber-energy system: Energy Internet[J]. Electric Power Automation Equipment,2016,36(9):1-7.

[3] US-Canada Power System Outage Task Force. Final report on the August 14,2003 blackout in the United States and Canada: causes and recommendations[R]. [S.l.]: U.S. Department of Energy, 2004.

[4] VANDENBERGHE F,GREBE E,KLAAR D,et al. Final report of the investigation committee on the 28 September 2003 blackout in Italy[R]. [S.l.]:UCTE,2004.

[5] 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.

[6] 叶夏明,文福拴,尚金成,等. 电力系统中信息物理安全风险传播机制[J]. 电网技术,2015,39(11):3072-3079.
YE Xiaming, WEN Fushuan, SHANG Jincheng, et al. Propagation mechanism of cyber physical security risks in power systems[J]. Power System Technology,2015,39(11):3072-3079.

[7] AMINIFAR F,FOTUHI-FIRUZABAD M,SHAHIDEHPOUR M,et al. Impact of WAMS malfunction on power system reliability assessment[J]. IEEE Transactions on Smart Grid,2012,3(3):1302-1309.

[8] 汤奕,李峰,王琦,等. 通信系统故障对电力系统实时负荷控制影响的量化评价方法[J]. 电力自动化设备,2017,37(2):90-96.
TANG Yi,LI Feng,WANG Qi,et al. Quantitative evaluation of communication system fault effect on real-time load control of power system[J]. Electric Power Automation Equipment, 2017, 37(2): 90-96.

[9] 曹一家,张宇栋,包哲静. 电力系统和通信网络交互影响下的连锁故障分析[J]. 电力自动化设备,2013,33(1):7-11.
CAO Yijia,ZHANG Yudong,BAO Zhejing. Analysis of cascading failures under interactions between power grid and communication network[J]. Electric Power Automation Equipment,2013,33(1): 7-11.

[10] 汤奕,韩啸,吴英俊,等. 考虑通信系统影响的电力系统综合脆弱性评估[J]. 中国电机工程学报,2015,35(23):6066-6074.
TANG Yi,HAN Xiao,WU Yingjun,et al. Considering the influence of communication system on the vulnerability assessment of electric power system[J]. Proceedings of the CSEE,2015,35(23):6066-6074.

[11] SRIVASTAVA A,MORRIS T,ERNSTER T,et al. Modeling cyber-physical vulnerability of the smart grid with incomplete information [J]. IEEE Transactions on Smart Grid,2013,4(1):235-244.

[12] 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.
[13] 冀星沛,王波,刘涤尘,等. 相依网络理论及其在电力信息-物理系统结构脆弱性分析中的应用综述[J]. 中国电机工程学报,2016,36(17):4521-4532.
JI Xingpei,WANG Bo,LIU Dichen,et al. Review on interdependent networks theory and its applications in the structural vulnerability analysis of electrical cyber-physical system[J]. Proceedings of the CSEE,2016,36(17):4521-4532.
[14] BULDYREV S V,PARSHANI R,PAUL G,et al. Catastrophic cascade of failures in interdependent networks[J]. Nature,2010,464(7291):1025-1028.
[15] 韩宇奇,郭创新,朱炳铨,等. 基于改进渗流理论的信息物理融合电力系统连锁故障模型[J]. 电力系统自动化,2016,40(17):30-37.
HAN Yuqi,GUO Chuangxin,ZHU Bingquan,et al. Modeling cascading failures in cyber physical power system based on improved percolation theory[J]. Automation of Electric Power Systems,2016,40(17):30-37.
[16] GUO J,HAN Y,GUO C,et al. Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties[J]. Energies,2017,10(1):87.
[17] ZHU Y,YAN J,SUN Y,et al. Revealing cascading failure vulnerability in power grids using risk-graph[J]. IEEE Transactions on Parallel and Distributed Systems,2014,25(12):3274-3284.
[18] 李志强,苏盛,曾祥君,等. 基于虚构诱骗陷阱的电力调度系统针对性攻击主动安全防护[J]. 电力系统自动化,2016,40(17):106-112.
LI Zhiqiang,SU Sheng,ZENG Xiangjun,et al. Fabricated traps based active cyber security defense against targeted cyber-attack in electric power dispatching systems[J]. Automation of Electric Power Systems,2016,40(17):106-112.
[19] 刘涤尘,冀星沛,陈果,等. 基于复杂网络理论的电力通信网加边保护策略[J]. 电力自动化设备,2016,36(10):121-126.
LIU Dichen,JI Xingpei,CHEN Guo,et al. Link addition strategy based on complex network theory for power communication network[J]. Electric Power Automation Equipment,2016,36(10):121-126.
[20] AN F,GAO X,GUAN J,et al. Modeling the interdependent network based on two-mode networks[J]. Physica A:Statistical Mechanics and its Applications,2017,483:57-67.
[21] 梅生伟,刘锋,魏韡. 工程博弈论基础及电力系统应用[M]. 北京:科学出版社,2016:454-458.
[22] DEB K,PRATAP A,AGARWAL S,et al. A fast and elitist multiobjective genetic algorithm:NSGA-Ⅱ[J]. IEEE Transactions on Evolutionary Computation,2002,6(2):182-197.
[23] 胡娟,李智欢,段献忠. 电力调度数据网结构特性分析[J]. 中国电机工程学报,2009,29(4):53-59.
HU Juan,LI Zhihuan,DUAN Xianzhong. Transmission characteristics analysis of the electric power dispatching data network[J]. Proceedings of the CSEE,2009,29(4):53-59.
[24] BARABASI A L,ALBERT R. Emergence of scaling in random networks[J]. Science,1999,286(5439):509-512.
[25] WATTS D J,STROGATZ S H. Collective dynamics of 'small-world' networks[J]. Nature,1998,393(6684):440-442.

作者简介:


张 殷

张 殷(1989—),男,河南南阳人,博士研究生,主要研究方向为电力系统安全分析(**E-mail**:zhangyin_scu@126.com);

肖先勇(1968—),男,四川宜宾人,教授,博士研究生导师,博士,通信作者,主要研究方向为不确定性理论在电力系统中的应用、电能质量、能源互联网、电力系统安全分析(**E-mail**:xiaoxianyong@163.com);

李长松(1973—),男,四川成都人,讲师,博士,主要研究方向为电力系统稳定与分析、智能供配电技术(**E-mail**:lcs21c@163.com)。

Vulnerability analysis of cyber physical power system from attacker's perspective

ZHANG Yin,XIAO Xianyong,LI Changsong

(College of Electrical Engineering and Information Technology,Sichuan University,Chengdu 610065,China)

Abstract:Analyzing the vulnerability of cyber physical power system from attacker's perspective is beneficial for decision makers to identify the vulnerable components and potential threats,which lays the foundation for the formulation of targeted defense. An integrated model of cyber physical power system considering the cyber physical interaction is built based on the complex network theory,and the impact of cyber component failures on the fault propagation of physical layer is studied under the DC power flow model. Four kinds of attack modes are proposed from the attacker's point of view,and the more comprehensive vulnerability indices of cyber physical power system are built from the perspectives of the structural and functional properties of physical and cyber layers to analyze the vulnerability of the system under two topologies of cyber network. Simulative results show that,the load level of physical layer and the topology of cyber layer are the important factors that affect the vulnerability of the system,compared with random attack modes,the system is more vulnerable under the malicious attack mode and especially vulnerable under the coordinated attack mode,the cyber nodes with high weighted betweenness and high weighted degree play a crucial role in maintaining the function of cyber layer,and the synergistic damage effect of cyber and physical component failures seriously deteriorates the system performance.

Key words:cyber physical power system;cyber physical interaction;complex network theory;vulnerability;attacker's perspective