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

阮 振[1],吕 林[1],刘友波[1],刘 捷[2],王电刚[2],黄 林[2]
(1. 四川大学 电气信息学院,四川 成都 610065;2. 国网四川省电力公司信息通信公司,四川 成都 610041)

摘要:随着电网信息层与物理层的耦合程度越来越高,配合良好的信息物理协同攻击将对电网造成巨大的威胁。为了更好地保障电网的安全稳定运行,在信息物理高度融合的背景下,提出了一种考虑负荷数据虚假注入的双层协同攻击模型。以广泛应用的基于残差分析的不良数据检测原理为基础,制定网络攻击与物理攻击资源分配约束;以考虑权重的负荷削减期望为损失度量指标,给出了上层攻击者最大化损失和下层防御者最小化损失的具体模型及求解方案;基于修改的 IEEE 14 节点系统进行了定量分析,得到了不同状态下攻击者的最优攻击方案,为电网防御者在信息物理协同攻击威胁下制定新的防御方案提供参考。

关键词:电力信息物理系统;负荷重分配攻击;虚假数据注入;协同攻击;模型
中图分类号:TM 761 **文献标识码**:A DOI:10.16081/j.issn.1006-6047.2019.02.027

0 引言

作为关乎百姓民生、社会稳定和经济发展的重要基础设施,电力系统的安全稳定至关重要。因此,各国电力系统一直以来都是恐怖分子及敌对势力的重要攻击目标。传统电力系统攻击主要分为如下 2 类:①物理攻击,以电力系统的一次设备为目标,攻击电网发电厂、输电线路和变电站等设施,破坏电网的网架结构,直接造成负荷损失甚至网络崩溃;②网络攻击,以电力系统的二次设备为目标,修改或盗取电网监测、控制、调节、保护等数据,间接获取经济利益或造成负荷损失,破坏电网的稳定[1]。

在世界范围内,电力系统遭受攻击的事件时有发生。近年来,巴基斯坦、乌克兰及以色列等地电网均遭受过物理或网络攻击[2]。物理攻击能直接破坏电网的网架结构,破坏力强,且易于检测。大量研究表明,当电网遭受物理攻击时,即使攻击部位的传感器已经失效,电网运行人员仍然能够及时发现故障,并采取相应的措施防止损失扩大。网络攻击在合理选择攻击向量后,隐蔽性强、不易检测,但单纯网络攻击的破坏力相对较弱[3]。

随着智能电网的不断发展,智能设备大量接入,电力系统的自动化程度越来越高,物理系统与信息系统的耦合程度也越来越深,逐渐形成了具备信息物理融合系统 CPS(Cyber-Physical System)典型特征的电力 CPS。电力 CPS 通过对电力系统进行全面详细的感知与分析,实现了合理的动态控制。然而新的技术也带来了新的挑战,传统电力系统设计之初并没有充分考虑到网络的安全因素,因此物理系统与信息系统的深度融合使得传统物理攻击及网络攻击能够协同作用,给电网带来了新的安全隐患[4-5]。

目前关于信息物理协同攻击的研究受到各国学者的广泛关注。一种研究思路是基于图论思想对电力 CPS 进行整体性安全分析,如文献[6-8]分别采用改进攻击图模型、改进渗流理论及社团理论对电力 CPS 进行脆弱性评估,实现了量化脆弱性、模拟实际连锁故障及大幅减少计算量等效果。此类模型从整体视角出发,在评估电力 CPS 跨空间连锁故障时具有很高的优越性,然而对于具体的攻击场景考虑较少。另一种研究思路是考虑具体的攻击场景,从电网防御者的角度展开研究,如文献[9]利用博弈论思想,分别建立了双层及三层模型,考虑了蓄意的信息物理协同攻击威胁下的最优防御方案,为电网运行人员进行防御资源配置提供了参考。但此类研究大多难以覆盖所有类型的攻击方法,如遭受网络攻击后大多只考虑信息节点失效而切负荷拒动等,未考虑如虚假数据注入攻击 FDIA(False Data Injection Attack)等其他类型的网络攻击对物理攻击的辅助效果。文献[10]提出了一种双层模型,计算了总攻击资源一定时最具破坏力的不可检测网络物理协同攻击方案。文献[11]讨论了攻击者利用不完全电网的网络信息制定不可检测的协同攻击方案。文献[12]考虑同步相量测量装置(PMU)的大量接入,分析了 FDIA 如何协同物理攻击绕过不良数据检测(BDD)装置。文献[13]首次讨论了一种特殊的 FDIA——负荷重分配(LR)攻击,这种网络攻击通过使电网运行人员错误地掌握网络的负荷分配而做出错误的调度决策,继而引发严重的后果。文献[14-16]对 LR 攻击进行了进一步的研究,文献[14]从即时攻击和延时攻击两方面定量分析了 LR 攻击对电力系统安全运行的危害;文献[15]讨论了攻击者不完全掌握网络信息时 LR 攻击的隐蔽性及危害;文献[16]基于半马尔科夫链建模,对电网进行了 LR 攻击下的可靠性评估。

收稿日期:2018-05-23;**修回日期**:2018-11-19
基金项目:国家自然科学基金资助项目(81437003)
Project supported by the National Natural Science Foundation of China(81437003)

现有文献大多关注LR攻击本身的研究,在LR攻击对电力系统的危害研究中也大多局限于探索具有最大危害的LR向量的选取上,对于具体的LR攻击与物理攻击协同攻击场景的研究较少。本文基于攻方视角,重点考虑了LR攻击与物理攻击协同作用时对电力CPS脆弱性的影响。首先,以基于残差检测的FDIA检测机理为基础,分析了实际情况中攻击者不完全掌握网络结构时网络攻击资源分配约束及物理攻击资源分配约束;然后,以攻击者在攻击资源一定时企图最大化电网损失的思路为基础建立上层模型,下层模型中一次物理系统以直流最优潮流建模,分析了在一定的攻击资源下,线路攻击、发电机攻击和LR攻击协同攻击的具体攻击场景中电网调度人员最小化损失的最优调度方案;最后,对双层模型进行求解,得到攻击者可能的最优攻击方案,为电网防御者提供重要的参考。

1 FDIA模型

文献[17]首次发现了电力系统错误数据检测算法的漏洞,并提出了FDIA。FDIA一经提出便受到了国内外学者的广泛关注[18]。在实际电力系统中,由于数据采集与监控(SCADA)系统在获取数据时易受到各种随机干扰或出现偶然故障,原始数据中不可避免地会出现不良数据。为了消除不良数据对状态估计的影响,以残差分析为基础的不良数据检测方法得到了广泛的应用。

1.1 理想攻击模型

FDIA最初在简单的线性直流系统中被发现,且被逐步引入复杂的交流系统。在一个具有N条母线的电力系统中,若采用直流模型,忽略线路电阻,则测量值(支路有功潮流和节点注入有功功率)和状态变量(母线相角)的关系满足:

$$\boldsymbol{z}=\boldsymbol{H}\boldsymbol{x}+\boldsymbol{e} \tag{1}$$

其中,$\boldsymbol{z}=[z_1,z_2,\cdots,z_m]^{\mathrm{T}}$为测量值向量,$\boldsymbol{x}=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$为状态变量,$n=2N-1$,$m>n$;$\boldsymbol{H}$为测量雅可比矩阵,只与支路电抗有关;$\boldsymbol{e}=[e_1,e_2,\cdots,e_m]^{\mathrm{T}}$为测量误差,根据统计规律其服从均值为0、方差为对角矩阵$\boldsymbol{R}=\mathrm{diag}(\sigma_1^2,\sigma_2^2,\cdots,\sigma_m^2)$的正态分布。给定测量值向量$\boldsymbol{z}$后,基于加权最小二乘法的目标函数为:

$$\min J(\boldsymbol{x})=(\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x})^{\mathrm{T}}\boldsymbol{R}^{-1}(\boldsymbol{z}-\boldsymbol{H}\boldsymbol{x}) \tag{2}$$

目标函数$J(\boldsymbol{x})$对状态变量$\boldsymbol{x}$的导数为0,即:

$$\partial J(\boldsymbol{x})/\partial \boldsymbol{x}\big|_{\boldsymbol{x}=\hat{\boldsymbol{x}}}=0 \tag{3}$$

则可得到状态变量$\boldsymbol{x}$的估计值$\hat{\boldsymbol{x}}$为:

$$\hat{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{R}^{-1}\boldsymbol{z} \tag{4}$$

由测量值向量的估计值$\hat{\boldsymbol{z}}=\boldsymbol{H}\hat{\boldsymbol{x}}$、残差$\boldsymbol{r}=\boldsymbol{z}-\hat{\boldsymbol{z}}$,得到残差的表达式为:

$$\boldsymbol{r}=\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}} \tag{5}$$

目前广泛采用的不良数据检测方法实质上是通过判断残差$\boldsymbol{r}$的2-范数$\|\boldsymbol{r}\|$是否大于门槛值τ,来检测测量值向量$\boldsymbol{z}$中是否含有不良数据。在FDIA中,攻击者向原始测量值向量中注入非零攻击向量$\boldsymbol{a}=[a_1,a_2,\cdots,a_m]^{\mathrm{T}}$,使得实际测量数据$\boldsymbol{z}_{\mathrm{bad}}=\boldsymbol{z}+\boldsymbol{a}$,令$\boldsymbol{c}=[c_1,c_2,\cdots,c_m]^{\mathrm{T}}$为此时的误差向量,则状态变量估计值$\hat{\boldsymbol{x}}_{\mathrm{bad}}=\hat{\boldsymbol{x}}+\boldsymbol{c}$。FDIA后的残差$\boldsymbol{r}_{\mathrm{a}}$的2-范数为:

$$\begin{aligned}\|\boldsymbol{r}_{\mathrm{a}}\|&=\|\boldsymbol{z}_{\mathrm{bad}}-\boldsymbol{H}\hat{\boldsymbol{x}}_{\mathrm{bad}}\|=\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{H}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|=\\&\quad\|\boldsymbol{z}-\boldsymbol{H}\hat{\boldsymbol{x}}+\boldsymbol{a}-\boldsymbol{H}\boldsymbol{c}\|\end{aligned} \tag{6}$$

故当攻击者完全掌握网络参数$\boldsymbol{H}$时,在简单的线性直流系统中,可通过合理选择攻击向量$\boldsymbol{a}=\boldsymbol{H}\boldsymbol{c}$,使攻击前、后残差的2-范数$\|\boldsymbol{r}\|$保持不变,从而成功避开基于残差分析的不良数据检测。

1.2 实际攻击模型

实际的状态估计模型几乎全部基于非线性交流系统,且攻击者难以完全掌握电力系统的全部信息。本节基于实际攻击模型分析FDIA躲避不良数据检测的原理,并给出LR攻击与攻击资源分配的关系。

类比理想模型,在给定网络拓扑、支路参数、测量值向量$\boldsymbol{z}=[z_1,z_2,\cdots,z_m]^{\mathrm{T}}$、状态变量$\boldsymbol{x}=[x_1,x_2,\cdots,x_n]^{\mathrm{T}}$时,含$N$条母线的电力系统状态估计的非线性量测方程为:

$$\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e},\ \boldsymbol{e}\sim\mathrm{N}(0,\boldsymbol{R}) \tag{7}$$

其中,$\boldsymbol{h}(\boldsymbol{x})$为非线性量测函数向量。攻击向量$\boldsymbol{a}=[a_1,a_2,\cdots,a_m]^{\mathrm{T}}$,实际测量数据$\boldsymbol{z}_{\mathrm{bad}}=\boldsymbol{z}+\boldsymbol{a}$,$\boldsymbol{c}=[c_1,c_2,\cdots,c_m]^{\mathrm{T}}$为状态估计值的偏差向量,则状态变量估计值$\hat{\boldsymbol{x}}_{\mathrm{bad}}=\hat{\boldsymbol{x}}+\boldsymbol{c}$。FDIA后的残差$\boldsymbol{r}_{\mathrm{a}}$的2-范数为:

$$\begin{aligned}\|\boldsymbol{r}_{\mathrm{a}}\|&=\|\boldsymbol{z}_{\mathrm{bad}}-\boldsymbol{h}(\hat{\boldsymbol{x}}_{\mathrm{bad}})\|=\\&\quad\|\boldsymbol{z}+\boldsymbol{a}-\boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c})+\boldsymbol{h}(\hat{\boldsymbol{x}})-\boldsymbol{h}(\hat{\boldsymbol{x}})\|\leqslant\\&\quad\|\boldsymbol{z}-\boldsymbol{h}(\hat{\boldsymbol{x}})\|+\|\boldsymbol{a}-\boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c})+\boldsymbol{h}(\hat{\boldsymbol{x}})\|=\\&\quad\|\boldsymbol{r}\|+\|\boldsymbol{a}-\boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c})+\boldsymbol{h}(\hat{\boldsymbol{x}})+\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}}+\boldsymbol{c})-\\&\quad\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}}+\boldsymbol{c})+\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}})-\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}})\|\leqslant\\&\quad\|\boldsymbol{r}\|+\|\boldsymbol{a}-\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}}+\boldsymbol{c})+\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}})\|+\delta\end{aligned} \tag{8}$$

其中,$\boldsymbol{h}'$为攻击者获取的网络参数的误差向量;$\hat{\boldsymbol{x}}_{\mathrm{error}}$为攻击者获取的状态变量估计值向量;$\delta$为信息不确定参数,满足式(9)。

$$\delta=\|\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}}+\boldsymbol{c})-\boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c})\|+\|\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}})-\boldsymbol{h}(\hat{\boldsymbol{x}})\| \tag{9}$$

要成功躲避不良数据检测,需满足$\|\boldsymbol{r}_{\mathrm{a}}\|\leqslant\tau$,即$\|\boldsymbol{a}-\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}}+\boldsymbol{c})+\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}})\|+\delta\leqslant\tau-\|\boldsymbol{r}\|$。当$\boldsymbol{a}$满足$\boldsymbol{a}=\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}}+\boldsymbol{c})+\boldsymbol{h}'(\hat{\boldsymbol{x}}_{\mathrm{error}})$时,$\|\boldsymbol{r}_{\mathrm{a}}\|$取最小值。由$\hat{\boldsymbol{z}}=\boldsymbol{h}(\hat{\boldsymbol{x}})$可知,状态估计值的偏差越大,则量测估计值的偏差也越大。要使攻击成功躲避不良数据检测,$\boldsymbol{h}'$与$\hat{\boldsymbol{x}}_{\mathrm{error}}$的偏差不能太大,而由式(9)可知,实际模型中$\boldsymbol{h}(\boldsymbol{x})$、$\boldsymbol{h}'(\boldsymbol{x})$基于交流系统建模,在$\boldsymbol{h}'$与$\hat{\boldsymbol{x}}_{\mathrm{error}}$的偏差不太大的情况下,满足二次关系,则$\delta$近似满足与状态估计值的偏差向量$\boldsymbol{c}$呈一次正相关,即状

态估计值与量测估计值的偏差越大,则要成功躲避不良数据检测的难度越高,且满足一次相关性。

2　攻击资源分配约束

考虑到实际情况中电网攻击者具有的攻击资源通常是有限的,以 R_{C}、R_{P} 分别表示电网攻击者具备的网络和物理攻击资源。由第 1 节可知,攻击者在某一节点分配足够的网络攻击资源后,FDIA 能够成功发动且避开不良数据检测。在物理攻击中,提高某一元件上的物理攻击资源,将会影响该元件的脆弱性,即提高该元件遭受攻击后失效的概率[9]。

2.1　LR 攻击资源分配约束

LR 攻击是一种特殊的 FDIA,其通过入侵电网各节点的 SCADA 等量测采集系统,修改负荷的分配,使电网调度人员错误地掌握电网节点的注入功率,从而在正常运行时做出错误的经济调度决策,在系统发生故障时导致更大的负荷削减甚至连锁故障。在 LR 攻击中,要躲避不良数据检测而成功发动攻击,根据第 1 节中的实际攻击模型建模,需考虑攻击者不完全掌握网络信息及测量值误差等因素[15]。本文以协同攻击场景为研究重点,仅以网络攻击资源约束描述攻击者的可攻击范围。由第 1 节的推导可知,量测值偏差大小与攻击难度正相关且近似满足一次相关性,即在限定网络攻击总资源 R_{C} 一定时,攻击节点的 LR 满足:

$$\sum_{i=1}^{N_{\mathrm{D}}}\left(C_{1,i}\left|\Delta P_{\mathrm{D},i}/P_{\mathrm{D},i}\right|+C_{2,i}\lambda_i\right)\leqslant R_{\mathrm{C}} \tag{10}$$

其中,N_{D} 为系统总节点数;$P_{\mathrm{D},i}$ 为节点 i 的有功负荷;$\Delta P_{\mathrm{D},i}$ 为节点 i 的 LR 有功功率,满足式(11)、(12)所示约束;$\boldsymbol{\lambda}=[\lambda_1,\lambda_2,\cdots,\lambda_{N_{\mathrm{D}}}]^{\mathrm{T}}$ 为判断 $\Delta P_{\mathrm{D},i}$ 是否为 0 的 N_{D} 维逻辑向量,具体取值情况如式(13)所示;$C_{1,i}$、$C_{2,i}$ 分别为入侵节点 i 随 $\Delta P_{\mathrm{D},i}$ 线性变化的 LR 攻击的投资参数和固定 LR 攻击的投资参数。

$$\sum_{i=1}^{N_{\mathrm{D}}}\Delta P_{\mathrm{D},i}=0 \tag{11}$$

$$-\chi P_{\mathrm{D},i}\leqslant\Delta P_{\mathrm{D},i}\leqslant\chi P_{\mathrm{D},i} \tag{12}$$

$$\Delta P_{\mathrm{D},i}=0\Rightarrow\lambda_i=0,\ \Delta P_{\mathrm{D},i}\neq0\Rightarrow\lambda_i=1\quad\forall i \tag{13}$$

其中,χ 为基于历史运行数据确定的常量[8],本文中 χ 取为 0.5。

2.2　物理攻击资源分配约束

本节考虑线路攻击和发电机攻击 2 类物理攻击。其中,输电线路分布于广泛区域内,容易遭受直接物理攻击,犯罪分子甚至有充分的时间逃离犯罪现场;而针对发电机的物理攻击,虽然难以直接发动,但可以通过误导调度人员,使其错误地掌握负荷需求等方法导致发电机跳闸[19]。以文献[20]中的攻击成功率函数对物理攻击资源分配与攻击成功概率关系进行建模。对于第 b 个物理目标,令 $A_{\mathrm{C}b}$ 为提高物理攻击成功概率的最低攻击投资,当攻击资源 $A_b\geqslant A_{\mathrm{C}b}$ 时,物理攻击成功概率 $p_b(A_b)$ 满足:

$$p_b(A_b)=1-\mathrm{e}^{-\beta_b A_b} \tag{14}$$

其中,A_b 为分配到第 b 个物理目标的物理攻击资源;$\beta_b=-\ln(1-p_{b0})/A_{\mathrm{C}b}$,$p_{b0}$ 为最低攻击投资时的攻击成功概率。当 $A_b<A_{\mathrm{C}b}$ 时,$p_b(A_b)=0$。令 $O\{b\}$ 为受到攻击且攻击成功而断路的物理目标(发电机或线路)集合,$O\{b'\}$ 为未受到攻击及受到攻击但攻击未成功的物理目标集合,$q_{O\{b\}}$ 为 $O\{b\}$ 中目标受攻击而其他目标未受攻击的概率,则 $q_{O\{b\}}$ 满足:

$$q_{O\{b\}}=\prod_{O\{b\}}p_b(A_b)\prod_{O\{b'\}}(1-p_{b'}(A_b)) \tag{15}$$

物理攻击总资源为 R_{P},则各物理目标的攻击资源分配满足:

$$\sum_{b=1}^{N_{\mathrm{P}}}A_b\leqslant R_{\mathrm{P}} \tag{16}$$

其中,N_{P} 为物理攻击目标数,本文中的物理目标考虑发电机和线路,即 $N_{\mathrm{P}}=N_{\mathrm{G}}+N_{\mathrm{F}}$,$N_{\mathrm{G}}$ 为系统中的发电机数,N_{F} 为线路数。

3　协同攻击双层优化模型及求解思路

现代电力系统的网架结构复杂,供电可靠性高,通常满足 $N-1$ 甚至 $N-2$ 准则。当系统正常运行时往往有充分的备用电源及线路容量,即使物理攻击成功发动,断开 1 条或多条线路(1 台或多台发电机),通过调度人员正确的应对,电网负荷损失很可能较小,甚至为 0。单纯发动 LR 攻击也难以对正常运行的电力系统造成大的损害。而 LR 攻击与物理攻击协同的攻击场景,通过 LR 攻击使调度人员错误地掌握负荷分配,做出错误的调度决策,使负荷转移到一小部分线路及发电机,而其他线路及发电机容量被大量浪费,进而使原本具有充分裕度的电网变得脆弱。此时,选取重载线路及发电机发动物理攻击,调度人员又错误地掌握系统的运行情况而无法做出正确的应对来减小损失,从而很可能造成电力系统较大的负荷损失甚至崩溃。

本节的协同攻击场景中,先由攻击者制定攻击方案,防御者在此攻击方案下采取合理的措施以减小损失。依此建立双层协同攻击优化模型,在防御者能做出最优调度方案的假设下,且攻击者的物理、网络攻击资源有限时,存在唯一的最优攻击方案。

3.1　双层优化模型

电网遭受攻击导致元件失效后,将有可能造成负荷削减、网络崩溃、设备返修、人员伤亡等各种损失。为了简化计算,本文仅以考虑权重的负荷削减作为衡量电网损失的指标。由于各个地区的负荷种

类及重要性不同,遭遇负荷削减后的综合损失也不相同。本文引入负荷权重向量 $\boldsymbol{\alpha}$,用 $\boldsymbol{\alpha}$ 与负荷削减 $\boldsymbol{P}_{\mathrm{C}}$ 的乘积表示电网的综合损失。

上层模型描述攻击者在网络攻击资源、物理攻击资源一定时,寻求最优的攻击策略给电网带来最大的损失。以考虑权重的负荷削减期望为目标函数:

$$L=\max\sum\left(q_{O\{b\}}\sum_{i=1}^{N_{\mathrm{D}}}P_{\mathrm{CO}\{b\},i}\alpha_i\right) \tag{17}$$

其中,L 为考虑权重的电网最大损失;$P_{\mathrm{CO}\{b\},i}$ 为 $O\{b\}$ 中物理目标受攻击而其他目标未受攻击,并且配合 LR 攻击后节点 i 的负荷削减;α_i 为节点 i 的负荷权重。约束条件包括:LR 攻击和物理攻击资源分配约束,$\Delta P_{\mathrm{D},i}$、$q_{O\{b\}}$ 与攻击资源的等式关系约束。即约束条件为式(10)—(16)。

下层模型描述电网防御者在遭受某特定的协同攻击后,根据掌握的电网信息,经合理的负荷削减调度,最大可能地减小攻击造成的损失。目标函数为:

$$\min\sum_{i=1}^{N_{\mathrm{D}}}P_{\mathrm{C},i}\alpha_i \tag{18}$$

其中,$P_{\mathrm{C},i}$ 为遭受一定攻击后的电网负荷损失。攻击参数由上层模型给出。此类电力 CPS 协同攻击大多针对大规模输电系统,采用直流潮流计算模型与交流潮流计算模型的误差不大,且在负荷削减计算过程中的精度要求相对较低,故为了方便计算,本节采用直流潮流模型对负荷削减进行建模。下层模型的约束条件如下:

$$\sum_{i=1}^{N_{\mathrm{D}}}P_{\mathrm{SP},i}=0 \tag{19}$$

$$P_{\mathrm{SP},i}=P_{\mathrm{G},i}-(P_{\mathrm{D},i}+\Delta P_{\mathrm{D},i}-P_{\mathrm{C},i})\quad i\in[1,N_{\mathrm{D}}] \tag{20}$$

$$\boldsymbol{F}=\boldsymbol{M}_{\mathrm{f}}\boldsymbol{B}^{-1}\boldsymbol{P}_{\mathrm{SP}} \tag{21}$$

$$-F_j^{\max}\leqslant F_j\leqslant F_j^{\max}\quad j\in[1,N_{\mathrm{F}}] \tag{22}$$

$$P_{\mathrm{G},k}^{\min}\leqslant P_{\mathrm{G},k}\leqslant P_{\mathrm{G},k}^{\max}\quad k\in[1,N_{\mathrm{G}}] \tag{23}$$

$$0\leqslant P_{\mathrm{C},i}\leqslant P_{\mathrm{D},i}\quad i\in[1,N_{\mathrm{D}}] \tag{24}$$

$$P_{\mathrm{G},k}^{\max}=P_{\mathrm{G},k}^{\max}-\eta_k P_{\mathrm{G},k}^{\max}\quad k\in[1,N_{\mathrm{G}}] \tag{25}$$

其中,式(19)、(20)为潮流等式约束,$P_{\mathrm{SP},i}$ 为节点 i 的注入功率,$P_{\mathrm{G},i}$ 为节点 i 的发电机有功出力;$\boldsymbol{F}$ 为支路潮流向量;$\boldsymbol{M}_{\mathrm{f}}$、$\boldsymbol{B}$ 分别为相应线路受攻击断开后的支路-节点关联的导纳矩阵和支路导纳矩阵;$\boldsymbol{P}_{\mathrm{SP}}$ 为节点注入功率向量;式(22)为支路潮流上下限约束,F_j 为第 j 条支路的潮流,$F_j^{\max}$ 为第 j 条支路的潮流上限;$P_{\mathrm{G},k}$ 为第 k 台发电机的出力;$P_{\mathrm{G},k}^{\max}$、$P_{\mathrm{G},k}^{\min}$ 分别为第 k 台发电机的出力上、下限;式(24)为负荷削减约束,节点负荷削减量不得大于该节点的实际负荷;式(25)为物理攻击后发电机的出力上限约束,η_k 为判断第 k 台发电机是否遭受攻击的逻辑变量。

3.2 求解策略

由于本文所建立的双层优化模型的上、下层之间存在耦合关系,且下层为线性模型,故采用遗传算法配合线性规划进行求解。在遗传算法中,初始化系统后,针对个体中的每一个变量,采用蒙特卡洛法在上下限之间进行抽样,随机生成父代种群,种群个体数目设置为 30。调用下层优化函数,由式(26)计算种群适应度。

$$f_{\mathrm{Fitness}}=\begin{cases}f(X) & X\text{ 为可行解}\\ f(X)+\sum K\Delta & X\text{ 为不可行解}\end{cases} \tag{26}$$

其中,X 为攻击策略;$f(X)$ 为下层优化结果;Δ 为不可行解与各约束条件上限的差值;K 为放大系数。通过多次交叉变异生成子代种群后,再次调用下层优化函数计算新的适应度并进行排序,保留精英,得出最优解。下层优化函数为混合整数线性规划模型,利用 yalmip 平台进行快速求解,其中参数 $\Delta P_{\mathrm{D},i}$、$\boldsymbol{M}_{\mathrm{f}}$、$\boldsymbol{B}$、$\eta_k$ 由上层模型给出。优化求解流程见图 1。

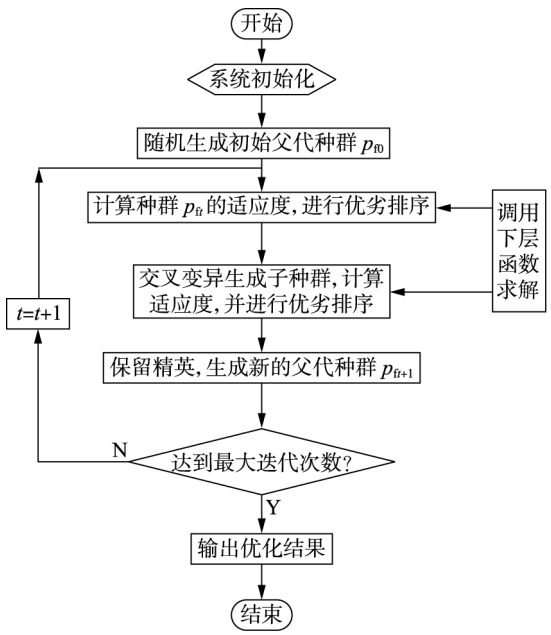


图 1 模型求解流程图

Fig.1 Flowchart of solving model

4 算例分析

4.1 参数设置

为了更好地体现本文模型的特征,以 IEEE 5 机 14 节点系统为例进行仿真,其接线图见图 2,并对部分参数进行了适当的修改。线路 1-2 的容量参数 $F^{\max}$ 设置为 160 MV·A,线路 2-3 的参数 $F^{\max}$ 设置为 100 MV·A,其他线路的参数 $F^{\max}$ 设置为 60 MV·A。其他参数从 MATPOWER 的 case14.m 文件中获取。依据系统正常运行时线路的负载大小确定线路的重要程度,设置线路的物理攻击参数如下:线路 1-2 的最低攻击投资参数 A_{C} 设置为 80,线路 2-3 的参数

A_C 设置为 60,线路 2-4 的参数 A_C 设置为 50,其他线路的参数 A_C 设置为 40。为了保证式(14)所示的攻击成功概率随攻击投资参数变化的合理性,所有线路的最低投资攻击成功概率 p_0 均设置为 0.8。发电机的容量参数、攻击投资参数见表 1,大容量机组的最低攻击投资参数 A_C 较大。各负荷节点的 LR 攻击投资参数 $C_{1,i}$、$C_{2,i}$及负荷权重参数 α_i 见表 2,大负荷节点的 LR 攻击投资参数较大,偏远地区的负荷权重较小。

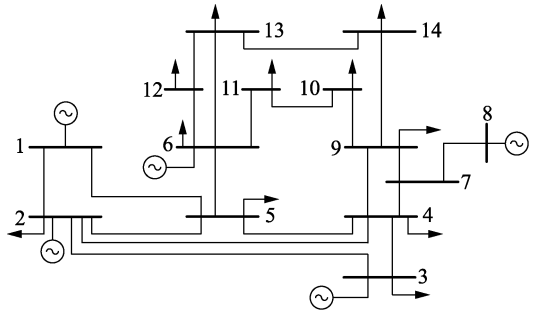


图 2　IEEE 5 机 14 节点系统

Fig.2　IEEE 5-machine 14-bus system

表 1　发电机参数

Table 1　Parameters of generators

所在节点	$P_{G,k}^{min}$/kW	$P_{G,k}^{max}$/kW	A_C	p_0
1	0	200	100	0.8
2	0	50	50	0.8
3	0	30	30	0.8
6	0	50	40	0.8
8	0	20	30	0.8

表 2　负荷参数

Table 2　Parameters of loads

节点	C_1	C_2	α/(MV·A)$^{-1}$	节点	C_1	C_2	α/(MV·A)$^{-1}$
2	2.5	1	1	10	2.5	1	0.8
3	7.5	3	1	11	2.5	1	0.8
4	5	2	1	12	2.5	1	0.8
5	2.5	1	0.9	13	2.5	1	0.8
6	2.5	1	0.9	14	2.5	1	0.8
9	5	2	0.9				

4.2　优化结果

本文分别选取电网在正常运行状态下和部分元件处于检修状态(即 $N-1$ 状态)下,物理攻击资源 R_P 为 40、60、80、100,网络攻击资源 R_C 为 0、10、20、30 时的最优协同攻击策略。

当电网处于正常运行状态时,以物理攻击资源 $R_P=40$ 为例,此时只能攻击 1 台 $A_C\leqslant 40$ 的发电机或 1 条 $A_C\leqslant 40$ 的线路。当受到网络资源攻击时,$L=0$,即单纯物理攻击不能给电网带来的损失;当 $R_C=10$,选择攻击线路 4-5,同时选取 LR 攻击向量 $\Delta\boldsymbol{P}_D=[0,-10.82,0,13.09,-3.36,0,0,0,0,1.07,0,0,0,0]^T$ MW 时的损失最大。LR 后节点的接线图见图 3。发动网络攻击将节点 2、5 的负荷转移到节点 4、10 上,同时断开节点 1、2 所连的 2 台主要出力机组和节点 4 的重要连接线路 4-5,此时调度人员根据对系统状态的掌握情况,优化得出最优调度方案为:削减节点 4 的负荷 $P_{C,4}=7.08$ MV·A。而以攻击方的视角,该攻击方案能对电网造成的最大损失 $L=5.67$。

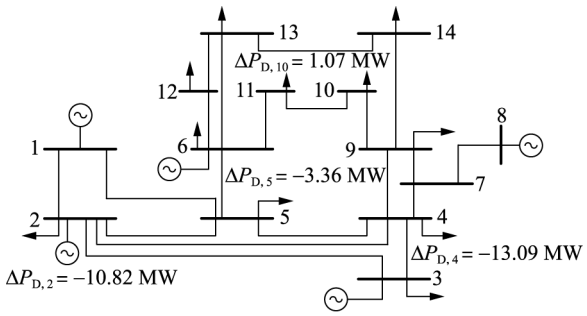


图 3　LR 后 IEEE 5 机 14 节点系统接线图

Fig.3　Wiring diagram of IEEE 5-machine 14-bus system under LR attack

当 R_C 较大时,能够通过攻击节点 3 处的发电机并配合网络攻击将其他节点的负荷转移到节点 3 或节点 3 附近的节点上,造成最大的损失。当物理攻击资源 $R_P=60$ 时,选择攻击线路 2-3 造成的损失最大,该损失随着协同攻击中网络攻击资源的增大而增大。当物理攻击资源 $R_P=80$、$R_C=0$,即单纯物理攻击时,选择攻击线路 1-2 造成的损失最大。随着网络攻击资源的增大,分别配合选取同时攻击节点 3 处的发电机、线路 2-4 及单独攻击线路 2-3 的物理攻击策略造成的损失最大。当物理攻击资源 $R_P=100$ 时,选择攻击节点 1 处的发电机造成的损失最大。正常运行状态下,电网最大损失 L 与网络攻击资源 R_C 及物理攻击资源 R_P 的关系曲线见图 4。

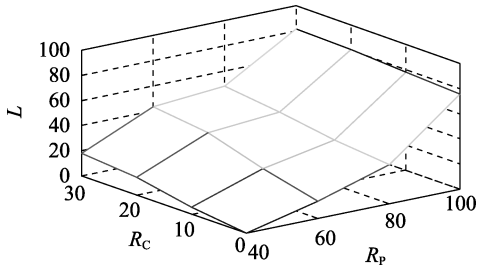


图 4　正常运行状态下 L 与 R_C 和 R_P 的关系曲线

Fig.4　Relationship curves of L vs. R_C and R_P under normal operation state

上述攻击策略中,除无负荷的节点 1、7、8 外,其他节点的 LR 有功功率 $\Delta P_{D,i}$ 的绝对值与节点 i 的实际有功负荷功率 $P_{D,i}$ 的比值的均值统计见图 5。某一节点的 $\Delta P_{D,i}/P_{D,i}$ 表示该节点遭受网络攻击的程度,由式(12)可知,本文中的 $\Delta P_{D,i}/P_{D,i}$ 最高不超过 0.5。对各种攻击情况下 $\Delta P_{D,i}/P_{D,i}$ 的均值进行统计,反映各节点在网络攻击下的脆弱性,$\Delta P_{D,i}/P_{D,i}$ 的均值越高,则网络遭受攻击的频率越高。由图 5

可知,正常运行状态下,负荷节点1、5、12、13在网络攻击中具有更高的脆弱性。当电网中某一物理元件处于检修状态,即电网处于$N-1$状态时,网络具有更高的脆弱性。本文选取节点2处发电机处于检修状态,计算各攻击资源下的最优攻击策略,结果见图6。$N-1$状态下$\Delta P_{D,i}/P_{D,i}$的均值分布见图7。

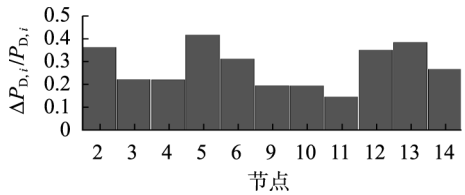


图5 正常运行状态下$\Delta P_{D,i}/P_{D,i}$的均值分布

Fig.5 Distribution of average $\Delta P_{D,i}/P_{D,i}$ under normal operation state

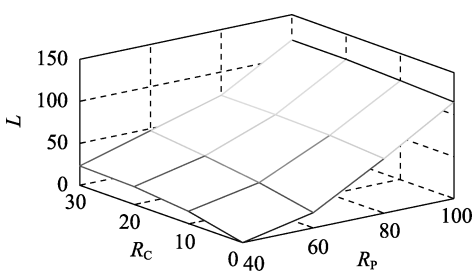


图6 $N-1$运行状态下L与R_C和R_P的关系曲线

Fig.6 Relationship curves of L vs. R_C and R_P under $N-1$ operation state

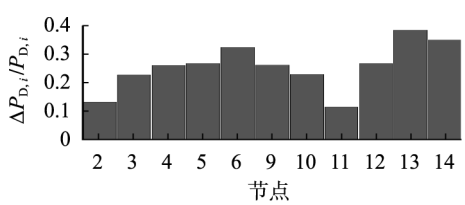


图7 $N-1$运行状态下$\Delta P_{D,i}/P_{D,i}$的均值分布

Fig.7 Distribution of average $\Delta P_{D,i}/P_{D,i}$ under $N-1$ operation state

由图4、6可知,信息物理协同攻击将对电网造成更大的损失,且当物理攻击资源一定时,损失随着网络攻击资源的增大而增大。在网络攻击的配合下,部分单纯物理攻击威胁中不太重要甚至允许发生故障的节点或线路变得至关重要。如在正常运行状态下当$R_P=40$时,对线路4-5或节点3处的发电机发动单纯物理攻击不会造成负荷损失,而配合网络攻击则会造成严重的损失;当$R_P=80$时,单纯物理攻击线路1-2造成的损失最大,而在协同攻击中,节点3处的发电机及线路2-3、2-4具有更高的脆弱性。与文献[5-7]中基于图论的模型相比,本文给出了具体的攻击方案及损失量化方法。与文献[8-9]中基于防御者视角模型相比较,本文考虑了新的协同攻击思路并通过$\Delta P_{D,i}/P_{D,i}$的均值分布计算,提供了各负荷节点在LR攻击下的脆弱性评估思路。

5 结论

本文在电网信息层与物理层高度耦合的背景下,定量分析了考虑负荷数据虚假注入的具体信息物理协同攻击场景。首先,基于FDIA模型给出了攻击资源分配约束;然后,以防御者最小化电网损失、攻击者最大化电网损失的思路,提出了双层攻击模型,并通过混合整数线性规划配合遗传算法进行求解;最后,通过算例计算了LR攻击与物理攻击配合下的电网综合损失,计算结果表明,在物理攻击资源有限的情况下,合理选择LR攻击向量的协同攻击将对电网造成巨大的威胁;同时给出了系统在2种运行状态下、攻击资源不同时攻击者可能的最优攻击策略及各负荷节点在网络攻击下的脆弱性,为电网防御者制定合理的防御策略提供了重要的依据。

由于实际电力CPS协同攻击中的影响因素众多,一、二次系统的交互复杂,本文在建模中做了许多简化,如损失建模中尚未考虑PMU等同步采集装置遭受攻击对系统稳定的影响及协同攻击可能带来的级联故障。下一阶段笔者将建立更精细的协同攻击模型并针对物理层、信息层提出具体的防御方案。

参考文献:

[1] SALMERON J, WOOD K, BALDICK R. Analysis of electric grid security under terrorist threat[J]. IEEE Transactions on Power Systems, 2004, 19(2): 905-912.

[2] 李中伟,佟为明,金显吉. 智能电网信息安全防御体系与信息安全测试系统构建乌克兰和以色列国家电网遭受网络攻击事件的思考与启示[J]. 电力系统自动化,2016,40(8):147-151.
LI Zhongwei, TONG Weiming, JIN Xianji. Construction of cyber security defense hierarchy and cyber security testing system of smart grid: thinking and enlightenment for network attack events to national power grid of Ukraine and Israel[J]. Automation of Electric Power Systems, 2016, 40(8): 147-151.

[3] 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):67-72,79.
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, 79.

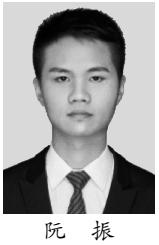
[4] 金波,肖先勇,李长松. 基于一、二次系统交互关系的电网连锁故障演化机制分析[J]. 电力自动化设备,2017,37(1):169-175.
JIN Bo, XIAO Xianyong, LI Changsong. Analysis of cascading failure evolution based on interaction between primary and secondary systems[J]. Electric Power Automation Equipment, 2017, 37(1): 169-175.

[5] 刘取,刘宪林. 21世纪电力系统的先进技术[J]. 电力自动化设备,2010,30(7):1-13,29.
LIU Qu, LIU Xianlin. Advanced technologies of power system in the 21st century[J]. Electric Power Automation Equipment, 2010, 30(7): 1-13, 29.

[6] 王宇飞,高昆仑,赵婷,等. 基于改进攻击图的电力信息物理系统跨空间连锁故障危害评估[J]. 中国电机工程学报,2016,36

(6):1490-1499.
WANG Yufei,GAO Kunlun,ZHAO Ting,et al. Assessing the harmfulness of cascading failures across space in electric cyber-physical system based on improved attack graph[J]. Proceedings of the CSEE,2016,36(6):1490-1499.
[7] 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. Model cascading failures in cyber physical power system based on improved percolation theory[J]. Automation of Electric Power Systems,2016,40(17):30-37.
[8] 汪勋婷,王波. 考虑信息物理融合的电网脆弱社团评估方法[J]. 电力自动化设备,2017,37(12):43-51.
WANG Xunting,WANG Bo. Assessment method of vulnerable communities in power grid considering cyber-physical integration[J]. Electric Power Automation Equipment,2017,37(12):43-51.
[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.
[10] LI Z Y,SHAHIDEHPOUR M,ALABDULWAHAB A,et al. Bilevel model for analyzing coordinated cyber-physical attacks on power systems[J]. IEEE Transactions on Smart Grid,2016,7(5):2260-2272.
[11] LI Z Y,SHAHIDEHPOUR M,ALABDULWAHAB A,et al. Analyzing locally coordinated cyber-physical attacks for undetectable line outages[J]. IEEE Transactions on Smart Grid,2018,9(1):35-47.
[12] DENG R L,ZHUANG P,LIANG H. CCPA:coordinated cyber-physical attacks and countermeasures in smart grid[J]. IEEE Transactions on Smart Grid,2017,8(5):2420-2430.
[13] YUAN Y L,LI Z Y,REN K. Modeling load redistribution attacks in power systems[J]. IEEE Transactions on Smart Grid,2011,2(2):382-390.
[14] YUAN Y L,LI Z Y,REN K. Quantitative analysis of load redistribution attacks in power systems[J]. IEEE Transactions on Parallel and Distributed Systems,2012,23(9):1731-1738.
[15] LIU X,BAO Z,LU D,et al. Modeling of local false data injection attacks with reduced network information[J]. IEEE Transactions on Smart Grid,2015,6(4):1686-1696.
[16] XIANG Y M,DING Z L,ZHANG Y C,et al. Power system reliability evaluation considering load redistribution attacks[J]. IEEE Transactions on Smart Grid,2016,8(2):889-901.
[17] LIU Y,REITER M K,NING P. False data injection attacks against state estimation in electronic power grids[J]. ACM Transactions on Information and System Security(TISSEC),2011,14(1):1-33.
[18] BI S Z,ZHANG Y J. Graphical methods for Defense against false-data injection attacks on power system state estimation[J]. IEEE Transactions on Smart Grid,2014,5(3):1216-1227.
[19] YINGMENG X,WANG L F,YU D,et al. Coordinated attacks against power grids:load redistribution attack coordinating with generator and line attacks[C]//2015 IEEE Power & Energy Society General Meeting. Denver,CO,USA:IEEE,2015:1-5.
[20] AL MANNAI W I,LEWIS T G. A general defender-attacker risk model for networks[J]. The Journal of Risk Finance,2008,9(3):244-261.

作者简介:


阮　振

阮　振(1992—),男,湖北武汉人,硕士研究生,主要研究方向为电力信息物理系统(**E-mail**:13258386832@163.com);

吕　林(1963—),男,四川成都人,教授,主要研究方向为电力系统分析(**E-mail**:lvlin@scu.edu.com);

刘友波(1983—),男,四川成都人,讲师,博士,主要研究方向为主动配电网规划与运行、电力信息物理系统等(**E-mail**:liuyoubo@scu.edu.com);

刘　捷(1973—),男,四川成都人,高级工程师,研究方向为电力系统信息通信;

王电刚(1973—),男,四川成都人,高级工程师,研究方向为电力系统自动化;

黄　林(1973—),男,四川成都人,高级工程师,研究方向为电力系统信息通信。

Coordinated attack model of cyber-physical power system considering false load data injection

RUAN Zhen[1],LÜ Lin[1],LIU Youbo[1],LIU Jie[2],WANG Diangang[2],HUANG Lin[2]
(1. School of Electrical Engineering and Information,Sichuan University,Chengdu 610065,China;
2. State Grid Sichuan Information and Communication Company,Chengdu 610041,China)

Abstract:With the increasing high coupling between the cyber layer and the physical layer in the power grid,a well cyber-physical coordinated attack will pose a tremendous threat to the power grid. Under this circumstance,a bi-level coordinated attack model considering the false load data injection is proposed to better ensure the safe and stable operation of the power grid. Based on the widely used residual analysis-based bad data detection principle,the resource allocation constraints of cyber attacks and physical attacks are formulated. The load reduction expectation considering weight is taken as a measure index of loss,and the concrete models and solutions for maximizing the losses of upper attacker and minimizing the losses of lower defenders are given. The quantitative analysis based on the modified IEEE 14-bus system is carried out. The optimal attack scheme of attackers under different states is obtained,which provides a reference for the power grid defenders to formulate the new defensive schemes under the threat of cyber-physical coordinated attacks.

Key words:cyber-physical power system;load redistribution attack;false data injection;coordinated attack;models