电力信息物理融合系统的网络-物理协同攻击

阳育德,蓝水岚,覃智君,刘 辉
(广西大学 电气工程学院,广西 南宁 530000)

摘要:随着智能电网的发展及智能设备不断引入电力信息物理融合系统(CPPS)中,CPPS面临一种新的攻击方式——网络-物理协同攻击(CCPAS)。这种攻击方式既隐蔽又可引发连锁故障,易造成大规模停电事故。首先,阐述CPPS遭受CCPAS的基本形式,在直流潮流模型下构建考虑状态估计约束的CCPAS模型。然后,探讨CCPAS的机理,以攻击者的角度分析规避状态估计监测后最大范围的攻击,分析CCPAS情景下CPPS的脆弱线路。最后,以IEEE 14、118节点系统为例,通过仿真计算验证模型的有效性、适用性,对比分析考虑状态估计约束后物理攻击的限制。

关键词:智能电网;信息物理融合系统;状态估计;网络-物理协同攻击;虚假数据注入攻击
中图分类号:TM 761 **文献标志码**:A DOI:10.16081/j.epae.202001004

0 引言

越来越多的智能控制设备、通信设备被引入传统的电力系统中,即信息系统与物理系统耦合构成的电力信息物理融合系统(CPPS),以更加高效、实时的方式监测或控制电网的物理设备或系统[1]。CPPS显著提升了电网的信息感知、集成、共享、协同能力。

但是,高级信息技术、设备的引入也给电力系统运行的可靠性、安全性带来潜在的隐患。近年来,对多个大停电事故的调查也证实信息系统的误操作或失效将会对电力系统的运行或监测产生显著影响[2]。2003年,北美输电物理系统与信息系统同时遭受攻击,状态估计、事故分析系统均未起作用[3]。2010年,发现了专门攻击电力控制系统或数据采集与监视控制(SCADA)系统的新型网络病毒——震网蠕虫Stuxnet。2015年,乌克兰输电线路连续跳闸,同时信息系统被植入恶意软件,阻挠了系统重启[4]。

在CPPS中,电力物理系统和信息系统的故障都可能导致大停电事故,目前学者大多将物理系统故障与信息系统故障分开研究。根据电力系统的静态安全规划,电力系统的输电系统可以承受N-1或者N-2故障运行,一旦系统的多条线路过载,极有可能引发连锁故障而导致大停电事故[5]。对于这类故障而言,在实际的生产过程中,即使在继电保护设备也发生故障的情况下,运行人员也能立即发现并采取控制措施以抑制故障的蔓延。电力信息系统的延迟、误码或中断将误导电力系统的控制策略,破坏电力系统的运行。网络攻击的方式主要有发送钓鱼邮件诱骗、植入恶意病毒以及注入虚假数据攻击[6-7]。

收稿日期:2019-01-03;**修回日期**:2019-11-11
基金项目:国家自然科学基金资助项目(51767001)
Project supported by the National Natural Science Foundation of China(51767001)

文献[8]基于电力系统的实时负荷控制代价量化评估通信系统故障对电力系统的影响。文献[9]基于改进图论算法进行信息的可达性分析,评估不可达信息可能造成的故障风险。文献[10]应用直流状态估计模型分析注入相量测量单元(PMU)的虚假数据,并规避了状态估计的检测。文献[11]在博弈论的基础上构造了物理与信息环节的攻防资源分配模型,量化分析了攻击过程中系统各环节的重要度。

除此之外,还有一类新的攻击方式——网络-物理协同攻击(CCPAS)层出不穷。CCPAS结合网络攻击来掩盖物理攻击造成的故障状态,既可以破坏物理系统的安全运行,又可延迟运行人员发现故障的时间,发起大规模的物理攻击,达到攻击者想要破坏系统安全稳定运行的目的。文献[12]结合复杂网络理论建立了信息物理交互的CPPS模型,在4种攻击模式下对比分析了CPPS物理层、信息层的脆弱性指标;结果表明基于完全信息攻击模式,CPPS在攻击者发起的信息-物理协同攻击下最为脆弱,信息-物理协同攻击可严重恶化系统的性能。文献[13]则分析了2种CCPAS模型:分别攻击发电机、输电线路与虚假数据注入攻击相结合,论证了CCPAS的潜在危害以及攻击的局限性。

文献[14]提出了考虑负荷数据虚假注入攻击与输电线路攻击的协同攻击情景,在重载线路发生故障与调度员错误掌握系统运行状态的双重攻击下可造成电力系统的崩溃。文献[15]通过电力系统可观测部分的参数等效构建电力系统不可观测部分的模型,构建以信息攻击掩盖物理攻击的CCPAS模型,使得电力系统故障状态不可检测。但故障状态的不可测约束仅仅考虑线路功率数据、节点数据的变量在合理的范围内,并没有考虑状态估计虚假数据检测作用,不能保证攻击完全隐秘。文献[16]通过改变电力系统测量仪表数据信息以及网络交换机数

据，以错误的网络信息误导控制中心，同时避免错误的数据信息被电力系统的状态估计识别。文献[17]提出掩盖输电线路故障的虚假数据需满足基尔霍夫电流、电压定律，并添加故障线路两端的数据残差，才能避免状态估计以及相量测量单元的检测。现有的协同攻击研究没有综合考虑物理攻击、信息攻击和避免状态估计的检测，也没有分析三者相互协同作用下的协同攻击后果以及具体的攻击模式。

本文建立了CCPAS模型，在物理系统侧，攻击者直接攻击输电线路，造成电力系统运行故障；在信息系统侧，攻击者利用虚假数据注入攻击、拓扑攻击掩盖系统的故障状态，同时避免状态估计的检测。协同攻击的隐秘性使故障不断蔓延，最终将导致电力系统崩溃。本文模型分析了输电线路断开的故障后果、相应注入的虚假数据及协同攻击中状态估计系统的抑制作用；考虑了状态估计的作用，表明攻击者的协同攻击虽不能无限扩大，但却更加完善、隐秘。

1 CCPAS的形式

随着智能电网的发展及越来越多的智能设备不断接入电力系统中，CPPS对智能设备的高度依赖及信息系统与物理系统的深度融合，使CPPS不再局限于受到电力系统物理侧的攻击或信息侧的网络攻击。

CCPAS结合了电力系统的物理系统攻击与信息系统的网络攻击：在物理系统侧，攻击者以电磁脉冲、狙击手的射击、飞行物干扰等手段攻击输电网的输电线路，导致多条线路过载跳闸；同时在信息系统侧，攻击者通过植入恶意软件、病毒或注入虚假数据，篡改系统的实时数据，致使信息系统通信错误的数据信息，掩盖系统的故障状态，使得运行人员未能及时发现系统的故障。

同时，网络攻击篡改的数据信息通过SCADA系统传送至控制中心的状态估计器中，篡改后的数据残差须在系统状态估计的有效值范围内，才能躲避状态估计的不良数据识别和辨识。

图1为CCPAS流程图。攻击者在电力系统的能源输送环节、监测环节同时发起攻击，既可直接破坏系统的正常运行，又可掩盖造成的故障，避开智能设备、运行人员的监测，这种攻击形式极有可能造成大规模的停电事故，严重破坏电力系统的安全稳定运行。

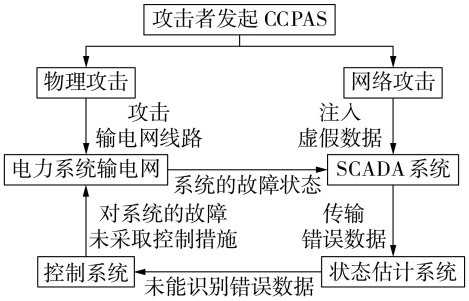

图1 CCPAS的流程图

Fig.1 Flowchart of CCPAS

2 CCPAS模型

2.1 物理攻击

在CCPAS的物理攻击中，应用直流潮流模型评估物理攻击造成断线后其余线路功率的变化量，即可根据输电线路断开后线路两端注入功率的变化，基于线路功率对节点注入功率的灵敏度矩阵，计算发生故障后其余线路的潮流变化。

基于PQ分解法的直流潮流方程，可推导得到支路线路有功功率与节点注入功率的关系为：

$$\boldsymbol{P}_l=\boldsymbol{T}_\Lambda^{-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{B}^{+}\boldsymbol{P} \tag{1}$$

$$\boldsymbol{P}_l=\boldsymbol{S}\boldsymbol{P} \tag{2}$$

其中，$\boldsymbol{P}$为节点注入功率向量；$\boldsymbol{P}_l$为支路l的有功功率潮流向量；$\boldsymbol{T}_\Lambda$为各支路电抗的对角阵；$\boldsymbol{A}$为网络关联矩阵；$\boldsymbol{B}^{+}$为节点导纳矩阵$\boldsymbol{B}$的穆尔-彭罗斯伪逆；$\boldsymbol{S}$为支路有功功率对节点注入功率的灵敏度矩阵。

所以物理攻击的数学模型可表示为：

$$\begin{cases}\Delta\boldsymbol{P}_l^{(1)}=-\sum\limits_{i\in N_{\mathrm{load}}}\boldsymbol{S}\Delta\boldsymbol{P}^{(1)}\\ \boldsymbol{P}_l^{(1)}=\mathrm{diag}\,(\boldsymbol{t}_l)(\boldsymbol{P}_l^{(0)}+\Delta\boldsymbol{P}_l^{(1)})\\ \Delta\boldsymbol{P}^{(1)}=\sum\limits_{l\in L,\,S_l\in N_{\mathrm{load}}}\boldsymbol{P}_l^{(1)}-\sum\limits_{l\in L,\,E_l\in N_{\mathrm{load}}}\boldsymbol{P}_l^{(1)}\end{cases} \tag{3}$$

其中，$\Delta\boldsymbol{P}^{(1)}$为物理攻击造成的节点注入功率的变化量；$\Delta\boldsymbol{P}_l^{(1)}$为注入线路$l$的功率虚假数据；$\boldsymbol{P}_l^{(0)}$、$\boldsymbol{P}_l^{(1)}$分别为初始状态下、物理攻击后系统线路$l$的有功功率向量；$S_l$、$E_l$分别为输电线路$l$的始端、末端节点号；$L$为系统的输电线路集合；$N_{\mathrm{load}}$为系统节点集合；$\boldsymbol{t}_l$为0-1变量向量，线路$l$断开时取值为1，未断开时取值为0。

2.2 物理攻击应避免造成网络孤点

攻击者攻击电力系统的输电网，断开系统多条关键线路，系统将可能形成孤岛运行。一旦形成孤岛运行，势必造成电力系统的功率不平衡，信息攻击将无法完全掩盖物理故障状态，运行人员发现故障后将立即实施相应的防御措施，从而导致攻击失败。因此，为了避免在攻击输电线路的过程中出现孤岛运行的情况，攻击者应保证整个系统的连通性，即每个节点至少连接1条线路。

在物理攻击过程中，保证不出现网络孤点运行的约束如下：

$$\begin{cases}\sum\limits_{l\in L,\,S_l=r}\boldsymbol{e}_l-\sum\limits_{l\in L,\,E_l=r}\boldsymbol{e}_l=(n-1)\boldsymbol{e}\\ \sum\limits_{l\in L,\,S_l\in R}\boldsymbol{e}_l-\sum\limits_{l\in L,\,E_l\in R}\boldsymbol{e}_l=-\boldsymbol{K}\\ -(n-1)(\boldsymbol{K}-\boldsymbol{t}_l)\leqslant\boldsymbol{e}_l\leqslant(n-1)(\boldsymbol{K}-\boldsymbol{t}_l)\end{cases} \tag{4}$$

其中，$\boldsymbol{e}_l$为整数变量，为输电线路上的虚拟电荷量；$\boldsymbol{e}$

为单位矩阵;$\boldsymbol{K}$为元素全是1的单位向量;r为选择的参考节点;R为其余节点集合;n为系统的节点总数。

在系统中选择1个节点为参考节点,从参考节点注入$n-1$个虚拟电荷量,剩余每个节点消纳1个单位电量,可保证每个节点至少连接有1条输电线路将1个电荷输送至该节点处,即可保证系统不会出现孤岛状态[18]。

2.3　注入虚假数据

虚假数据注入攻击,也称为负荷再分配攻击,是通过向分布在电网中的智能计量装置注入虚假数据,或者直接截取、篡改SCADA系统的数据包,误导电力系统控制中心的调度决策偏离实际状态,致使运行人员不能发现系统的故障。

发起虚假数据注入攻击的攻击者一般需要具备以下的条件:

(1)攻击者具有一定的电力专业知识,了解电力系统的运行结构、网络拓扑结构、状态估计原理等;

(2)攻击者具有一定的计算机专业知识,具备攻击智能装置并篡改数据信息的能力。

虚假数据注入攻击的数学模型可表示为:

$$\sum_{i\in N_{\text{load}}}\Delta\boldsymbol{P}^{(2)}=0,\quad \Delta\boldsymbol{P}_l^{(2)}=-\sum_{i\in N_{\text{load}}}\boldsymbol{S}\Delta\boldsymbol{P}^{(2)} \tag{5}$$

其中,$\Delta\boldsymbol{P}^{(2)}$为注入的虚假节点功率数据;$\Delta\boldsymbol{P}_l^{(2)}$为注入的虚假输电线路功率数据。

2.4　躲避状态估计识别的约束

经过状态估计辨识的数据直接用于潮流优化计算,因此状态估计的数据识别对电力系统的发电控制和经济调度有着直接的影响。即虚假数据注入攻击直接误导电力系统的信息决策,进而导致控制中心不能发现系统的故障,做出错误的控制措施[19-20]。

关于直流状态估计模型,记常数雅可比矩阵为$\boldsymbol{H}$;$\boldsymbol{Z}$为量测向量,包括节点注入功率、线路首端功率测量值、线路末端功率测量值;$\boldsymbol{x}$为状态变量向量,包括各节点电压相角;$\boldsymbol{W}$为量测量可信度的权重值,所取权重值越大,则量测精度越高,反之就越低。那么,基于加权最小二乘法的直流状态估计模型的目标函数为:

$$f(\boldsymbol{x})=(\boldsymbol{Z}-\boldsymbol{H}\boldsymbol{x})^{\mathrm{T}}\boldsymbol{W}(\boldsymbol{Z}-\boldsymbol{H}\boldsymbol{x}) \tag{6}$$

要使目标函数$f(\boldsymbol{x})$达到最小值,状态估计量$\bar{\boldsymbol{x}}$必须满足极值条件,即:

$$\left.\frac{\mathrm{d}f(\boldsymbol{x})}{\mathrm{d}\boldsymbol{x}}\right|_{\boldsymbol{x}=\bar{\boldsymbol{x}}}=2\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}(\boldsymbol{Z}-\boldsymbol{H}\bar{\boldsymbol{x}})=0 \tag{7}$$

即可推导得到状态估计量$\bar{\boldsymbol{x}}$为:

$$\bar{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{Z} \tag{8}$$

量测误差是服从均值为0、方差为σ^2的正态分布的随机向量,量测量的权重值通常以测量误差方差的倒数$1/\sigma^2$表示。根据文献[21],误差在$[-\sigma,\sigma]$范围外的量测被认为是不良数据,其值一般是在正常量测范围的0.5%~2%。

攻击者注入的虚假数据信息必须被状态估计接受,才能有效地躲避不良数据的检测和辨识。系统的量测量取节点有功功率数据以及输电线路两端有功功率数据,状态量为节点电压相角数据,即:

$$\begin{cases}\boldsymbol{P}_l^{(3)}=\boldsymbol{P}_l^{(0)}+\Delta\boldsymbol{P}_l^{(1)}+\Delta\boldsymbol{P}_l^{(2)}\\ \boldsymbol{P}^{(3)}=\boldsymbol{P}^{(0)}+\Delta\boldsymbol{P}^{(1)}+\Delta\boldsymbol{P}^{(2)}\\ \boldsymbol{Z}=[\boldsymbol{P}^{(3)};\boldsymbol{P}_l^{(3)};-\boldsymbol{P}_l^{(3)}]\end{cases} \tag{9}$$

其中,$\boldsymbol{P}_l^{(3)}$为注入虚假数据后各支路有功功率向量;$\boldsymbol{P}^{(3)}$为注入虚假数据后各节点的有功功率向量。

所以CCPAS躲避系统状态估计的约束为:

$$\begin{cases}\bar{\boldsymbol{x}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{W}\boldsymbol{Z}\\ \bar{\boldsymbol{Z}}=\boldsymbol{H}\bar{\boldsymbol{x}}\\ -\varepsilon_{\mathrm{c}}\left|\boldsymbol{Z}^{(0)}\right|\leqslant\boldsymbol{Z}-\bar{\boldsymbol{Z}}\leqslant\varepsilon_{\mathrm{c}}\left|\boldsymbol{Z}^{(0)}\right|\\ \alpha\boldsymbol{P}^{(0)}\leqslant\Delta\boldsymbol{P}^{(1)}+\Delta\boldsymbol{P}^{(2)}\leqslant\beta\boldsymbol{P}^{(0)}\\ \alpha\left|\boldsymbol{P}_l^{(0)}\right|\leqslant\Delta\boldsymbol{P}_l^{(1)}+\Delta\boldsymbol{P}_l^{(2)}\leqslant\beta\left|\boldsymbol{P}_l^{(0)}\right|\end{cases} \tag{10}$$

其中,$\bar{\boldsymbol{Z}}$为量测量的估计值;ε_{c}为状态估计量测误差的阈值;α、β分别为注入的虚假数据安全下界、上界。

3　模型求解

本文的CCPAS模型为攻击者发起物理攻击并配合攻击少量信息数据的具体数学模型。攻击者可以根据物理攻击方案破坏电力系统的运行,根据虚假数据注入的数据信息攻击信息系统的信息从而掩盖故障状态,使得运行人员无法发现电力系统的故障,致使故障不断蔓延。所以,协同攻击的目标函数为物理系统输电线路有功功率变化量之和最大,即从攻击者视角计算协同攻击可造成的故障严重度。

目标函数f可表示为式(11),即本文所建立的CPPS的CCPAS模型为式(3)—(5)、(9)、(10),是含有0-1变量的混合整数非线性规划模型,为了求解方便,需将模型中的非线性约束条件转为线性约束,即将模型转为混合整数线性规划模型。

$$f=\max\left\{\sum_{l\in L}\left|\Delta\boldsymbol{P}_l^{(1)}\right|(\boldsymbol{K}-\boldsymbol{t}_l)\right\} \tag{11}$$

引入中间变量$\boldsymbol{u}_l$、$\Delta\boldsymbol{P}_l^{(1)+}$、$\Delta\boldsymbol{P}_l^{(1)-}$以及大数$M$,对目标函数中的绝对值做式(12)所示转换,从而去除目标函数中的绝对值。

$$\begin{cases}\left|\Delta\boldsymbol{P}_l^{(1)}\right|=\Delta\boldsymbol{P}_l^{(1)+}+\Delta\boldsymbol{P}_l^{(1)-}\\ \Delta\boldsymbol{P}_l^{(1)}=\Delta\boldsymbol{P}_l^{(1)+}-\Delta\boldsymbol{P}_l^{(1)-}\\ 0\leqslant\Delta\boldsymbol{P}_l^{(1)+}\leqslant M(\boldsymbol{K}-\boldsymbol{u}_l)\quad\forall l\in L\\ 0\leqslant\Delta\boldsymbol{P}_l^{(1)-}\leqslant M\boldsymbol{u}_l\\ [\boldsymbol{u}_l]\in\{0,1\}\end{cases} \tag{12}$$

故目标函数可写为:

$$f=\max\left\{\sum_{l\in L}\left(\Delta\boldsymbol{P}_l^{(1)+}+\Delta\boldsymbol{P}_l^{(1)-}-\boldsymbol{t}_l\Delta\boldsymbol{P}_l^{(1)+}-\boldsymbol{t}_l\Delta\boldsymbol{P}_l^{(1)-}\right)\right\} \tag{13}$$

引入变量$\boldsymbol{\rho}_l^+$、$\boldsymbol{\rho}_l^-$，将模型中的非线性项$\boldsymbol{t}_l\Delta\boldsymbol{P}_l^{(1)+}$、$\boldsymbol{t}_l\Delta\boldsymbol{P}_l^{(1)-}$转为线性项，如式(14)所示。

$$\begin{cases}\boldsymbol{\rho}_l^+=\boldsymbol{t}_l\Delta\boldsymbol{P}_l^{(1)+}\\ \boldsymbol{\rho}_l^-=\boldsymbol{t}_l\Delta\boldsymbol{P}_l^{(1)-}\\ -M\boldsymbol{t}_l\leqslant\boldsymbol{\rho}_l^+\leqslant M\boldsymbol{t}_l\\ -M\boldsymbol{t}_l\leqslant\boldsymbol{\rho}_l^-\leqslant M\boldsymbol{t}_l\\ \Delta\boldsymbol{P}_l^{(1)+}-M(\boldsymbol{K}-\boldsymbol{t}_l)\leqslant\boldsymbol{\rho}_l^+\leqslant\Delta\boldsymbol{P}_l^{(1)+}+M(\boldsymbol{K}-\boldsymbol{t}_l)\\ \Delta\boldsymbol{P}_l^{(1)-}-M(\boldsymbol{K}-\boldsymbol{t}_l)\leqslant\boldsymbol{\rho}_l^-\leqslant\Delta\boldsymbol{P}_l^{(1)-}+M(\boldsymbol{K}-\boldsymbol{t}_l)\end{cases} \tag{14}$$

综上可将目标函数f及物理攻击后的支路有功功率$\boldsymbol{P}_l^{(1)}$写为：

$$\begin{cases}f=\max\left\{\sum_{l\in L}(\Delta\boldsymbol{P}_l^{(1)+}+\Delta\boldsymbol{P}_l^{(1)-}-\boldsymbol{\rho}_l^+-\boldsymbol{\rho}_l^-)\right\}\\ \boldsymbol{P}_l^{(1)}=\boldsymbol{t}_l\boldsymbol{P}_l^{(0)}+\boldsymbol{\rho}_l^+-\boldsymbol{\rho}_l^-\end{cases} \tag{15}$$

经一系列的转换后，原混合整数非线性规划模型将转化为混合整数线性规划模型，利用MATLAB调用Gurobi求解器基于分支割平面法进行求解。

4 算例分析

为了验证本文所提CCPAS模型的正确性和有效性，以IEEE 14、IEEE 118节点系统为例进行仿真分析。仿真算例的测试环境为MATLAB的R2014a版本；硬件配置为Intel(R)Core(TM) i7-7700 CPU@3.60 GHz，内存容量为8 GB。

4.1 IEEE 14节点系统算例

假设IEEE 14节点系统输电线路1-2的容量为160 MW，其余线路的容量为80 MW，模型的其他预设参数[22]如下：$\alpha=-0.2$，$\beta=0.2$，$M=10^5$，$\varepsilon_c=0.02$。

首先，假设攻击方只攻击物理系统的1条线路，即在模型中添加约束$\mathrm{sum}(\boldsymbol{t}_l)=1$，可得IEEE 14节点系统的1条线路被攻击后系统线路功率的变化量，结果见附录中的表A1。

攻击者对电力系统发起物理攻击，造成线路1-5断线，导致线路4-5过载，同时发起网络攻击注入虚假数据，可将线路功率的变化完全掩盖，使反馈给状态估计系统的数据与故障前并无差别，即成功发起CCPAS。文献[22]构建了攻击成本最小、故障最严重的双目标协同攻击模型，在有限的攻击成本下分析了物理攻击的攻击方案、造成的故障后果及信息攻击的数据信息。当攻击成本为30时，文献[22]的攻击方案为攻击线路3-4，所用的攻击代价为28，故障的严重度为69 MW；本文的攻击方案为攻击线路1-5，故障的严重度为202.97 MW，按文献[22]计算攻击成本的方法计算本文方案的攻击成本，所得结果同样为28，即本文模型以同样的攻击成本求解的CCPAS方案对电力系统造成的故障更为严重。

考虑与不考虑状态估计约束时的攻击方案对比如表1所示。由表可知，当只断开1条线路时，考虑状态估计约束的目标函数值较未考虑状态估计约束的目标函数值小235.7 MW。不考虑攻击成本约束后，考虑状态估计约束的协同攻击方案最多只能攻击6条输电线路，并且故障的严重度为1 457.95 MW，即这是协同攻击的极限方案。由于状态估计的制约，协同攻击方案如果超过极限方案，虚假数据注入攻击将无法完全掩盖物理系统的故障状态，协同攻击将会被运行人员发现。

将考虑与不考虑状态估计约束的攻击方案与文献[22]中不考虑攻击成本约束的攻击方案进行对比，结果如表2所示。由表可见，攻击线路数越多，虽能对系统造成非常严重的故障，但是系统元件数据的变化越多，网络攻击注入的虚假数据就越难掩盖故障状态，协同攻击势必被状态估计识别。因此，本文建立的协同攻击模型主要分析利用注入虚假数据来掩盖物理系统的故障状态，并考虑协同攻击过程中状态估计的识别作用，确保协同攻击不被运行人员发现，使得故障不断蔓延。

综合IEEE 14节点系统的仿真结果可知：物理系统输电线路的故障可通过网络攻击注入虚假数据来掩盖电力系统的故障状态；故障线路增多，系统的故障情况越来越严重，网络攻击注入的虚假数据就不能完全掩盖电力系统的故障。

4.2 IEEE 118节点系统算例

IEEE 118节点系统在不同攻击方案下的目标函数对比如表3所示。由表可知，攻击线路数从1条逐渐增多，3种攻击方案下的目标函数都逐渐增加，即系统的故障状态不断蔓延。但是CCPAS受到状态估计约束的制约，攻击者的攻击遭受限制，不能发起更大规模的攻击。即状态估计在电力系统错误数据识别过程中发挥着重要的作用，在网络攻击的防御研究中将是重点研究内容。

一旦发生CCPAS，系统中的输电线路极有可能被利用，致使运行人员未能发现系统的故障，造成连锁故障以及大规模停电事故。电力系统的脆弱点不

表1 考虑与不考虑状态估计约束时的攻击方案对比

Table 1 Comparison of attack schemes between with and without state estimation constraints

$\mathrm{sum}(\boldsymbol{t}_l)$	考虑状态估计约束		不考虑状态估计约束	
	f/MW	断开的线路	f/MW	断开的线路
1	202.97	1-5	438.67	1-2
≤10	1457.95	2-3,2-4,2-5,4-5,6-11,7-9	1805.78	2-3,2-4,2-5,4-5,6-13,10-11,4-9

表 2　攻击方案的结果对比

Table 2　Results comparison among attack schemes

线路	$P_l^{(0)}$ / MW	$P_l^{(1)}$ / MW		
		考虑状态估计约束	不考虑状态估计约束	文献[22]方案
1-2	156.83	**327.67**	**327.67**	-18.3
1-5	75.56	-95.28	-95.28	**237.3**
2-3	73.18	—	—	—
2-4	56.13	—	—	—
2-5	41.52	—	—	—
3-4	-23.34	49.85	49.85	**-94.2**
4-5	-61.14	—	—	**-229.7**
6-11	7.26	—	10.96	-45.7
6-12	9.00	-44.00	**-201.84**	34.5
6-13	16.69	**-128.03**	—	—
7-8	0	0	0	0
7-9	28.03	—	**202.43**	**87.7**
9-10	5.32	-1.95	1.62	58.2
12-13	2.81	-50.19	**-208.03**	28.4
13-14	5.80	**-191.93**	**-188.36**	14.9
14-9	-9.16	**-209.88**	**-203.32**	—
10-11	-3.70	-10.96	—	49.2
4-7	28.03	56.06	**202.43**	**87.7**
4-9	16.06	**178.48**	—	—
5-6	44.16	**-146.30**	**-146.30**	—

注："—"表示对应的线路断开。

表 3　IEEE 118 节点系统在不同攻击方案下的目标函数值对比

Table 3　Comparison of objective function values of IEEE 118-bus system among different attack schemes

攻击的线路数/条	f / MW		
	考虑状态估计约束	不考虑状态估计约束	文献[22]方案
1	2029.83	2828.16	2814.48
2	3575.23	4263.47	4045.14
3	4058.32	4702.58	4833.32
4	4518.92	6819.31	9040.99

再局限于系统重负载的输电线路，系统的轻载、负荷少的线路也有可能被恶意利用，破坏系统的安全运行。因此在CPPS可靠运行研究中，不仅需要考虑物理系统重要的输电线路故障，还要综合考虑信息系统的故障以及CCPAS的可能。

5　结论

随着智能电网的发展及越来越多的智能设备被引入电力系统，CPPS物理侧、信息侧的漏洞更容易被网络黑客利用，使电力系统发生故障。在此背景下，本文针对电力系统遭受CCPAS的机理进行初步探讨。

针对CPPS的特点，本文建立的CCPAS模型考虑了状态估计的作用，攻击者的攻击策略受到虚假数据注入以及状态估计的制约，所得结论如下：

（1）随着攻击线路的增多，过载线路不断增多，系统的故障状态越严重，故障不断蔓延即可引发连锁故障；

（2）网络攻击通过注入相关虚假数据掩盖物理系统的故障状态；

（3）当攻击的线路过多时，由于系统状态估计的识别作用，注入的虚假数据并不能完全掩盖电力系统的故障，说明了状态估计在电力系统防御中的重要性。

鉴于攻击者不是电力系统的专业运行人员，不能准确获悉电力系统的网络参数、拓扑结构，不能把握电力系统的实时运行状态，因此本文所提CCPAS模型的系统故障后果约束、虚假数据注入攻击约束以及躲避状态估计识别约束均应用直流模型模拟。本文目前的工作尚处在初级阶段，只基于攻击方视角考虑了协同攻击中状态估计的作用以及协同攻击对电力系统造成的影响，对于CPPS如何识别系统遭受的CCPAS并及时做出相应的防御策略从而避免大停电事故的发生等问题还有待解决，在今后的科研工作中将进一步对CPPS的防御模型进行研究。

附录见本刊网络版（http://www.epae.cn）。

参考文献：

[1] 郭庆来，辛蜀骏，孙宏斌，等. 电力系统信息物理融合建模与综合安全评估：驱动力与研究构想[J]. 中国电机工程学报，2016，36(6)：1481-1489，1761.
GUO Qinglai，XIN Shujun，SUN Hongbin，et al. Power system cyber-physical modelling and security assessment：motivation and ideas[J]. Proceedings of the CSEE，2016，36(6)：1481-1489，1761.

[2] WADHAWAN Y，NEUMAN C，ALMAJALI A. Analyzing cyber-physical attacks on smart grid systems[C]//2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES). Pittsburgh，PA，USA：IEEE，2017：21.

[3] 周博文，陈麒宇，杨东升. 巴西大停电的思考[J]. 发电技术，2018，39(2)：97-105.
ZHOU Bowen，CHEN Qiyu，YANG Dongsheng. On the power system large-scale blackout in Brazil[J]. Power Generation Technology，2018，39(2)：97-105.

[4] 赵俊华，梁高琪，文福拴，等. 乌克兰事件的启示：防范针对电网的虚假数据注入攻击[J]. 电力系统自动化，2016，40(7)：149-151.
ZHAO Junhua，LIANG Gaoqi，WEN Fushuan，et al. Lessons learnt from Ukrainian blackout：protecting power grids against false data injection attacks[J]. Automation of Electric Power Systems，2016，40(7)：149-151.

[5] 王韶，刘沛铮，董光德，等. 基于复杂网络理论计及校正控制的电力系统连锁故障模型[J]. 电力自动化设备，2016，36(9)：162-168.
WANG Shao，LIU Peizheng，DONG Guangde，et al. Power system cascading failure model based on complex network theory，with consideration of corrective control[J]. Electric Power Automation Equipment，2016，36(9)：162-168.

[6] DENG R L，XIAO G X，LU R X. Defending against false data injection attacks on power system state estimation[J]. IEEE Transactions on Industrial Informatics，2017，13(1)：198-207.

[7] 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.

[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] 郭采珊,蔡泽祥,潘天亮,等. 基于信息可达性的智能变电站继电保护系统风险评估方法[J]. 电网技术,2018,42(9):3041-3048.
GUO Caishan, CAI Zexiang, PAN Tianliang, et al. Risk assessment for protection system in smart substation considering information reachability[J]. Power System Technology, 2018, 42(9): 3041-3048.

[10] 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.

[11] 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.

[12] 张殷,肖先勇,李长松. 基于攻击者视角的电力信息物理融合系统脆弱性分析[J]. 电力自动化设备,2018,38(10):81-88.
ZHANG Yin, XIAO Xianyong, LI Changsong. Vulnerability analysis of cyber physical power system from attacker's perspective[J]. Electric Power Automation Equipment, 2018, 38(10): 81-88.

[13] XIANG Y M, WANG L F, LIU N. Coordinated attacks on electric power systems in a cyber-physical environment[J]. Electric Power Systems Research, 2017, 149: 156-168.

[14] 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, LÜ 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.

[15] 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.

[16] KIM J, TONG L. On topology attack of a smart grid: undetectable attacks and countermeasures[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(7): 1294-1305.

[17] LIU X, LI Z Y, LIU X D, et al. Masking transmission line outages via false data injection attacks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(7): 1592-1602.

[18] FAN N, IZRAELEVITZ D, PAN F, et al. A mixed integer programming approach for optimal power grid intentional islanding[J]. Energy Systems, 2012, 3(1): 77-93.

[19] 朱杰,张葛祥,王涛,等. 电力系统状态估计欺诈性数据攻击及防御综述[J]. 电网技术,2016,40(8):2406-2415.
ZHU Jie, ZHANG Gexiang, WANG Tao, et al. Overview of fraudulent data attack on power system state estimation and defense mechanism[J]. Power System Technology, 2016, 40(8): 2406-2415.

[20] BEG O A, JOHNSON T T, DAVOUDI A. Detection of false-data injection attacks in cyber-physical DC microgrids[J]. IEEE Transactions on Industrial Informatics, 2017, 13(5): 2693-2703.

[21] 于尔铿. 电力系统状态估计[M]. 北京:水利电力出版社,1985:110-116.

[22] 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.

作者简介:


阳育德

阳育德(1971—),男,广西桂林人,副教授,博士,研究方向为电力系统优化理论及其计算(**E-mail**:yangyude@gxu.edu.cn);

蓝水岚(1991—),女,广西河池人,硕士研究生,主要研究方向为电力信息物理融合系统可靠性分析(**E-mail**:381730626@qq.com)。

(**编辑** 陆丹)

Coordinated cyber-physical attacks of cyber-physical power system

YANG Yude, LAN Shuilan, QIN Zhijun, LIU Hui

(School of Electrical Engineering, Guangxi University, Nanning 530000, China)

Abstract: With the development of smart grid and the continuous introduction of smart devices into CPPS (Cyber-Physical Power System), CPPS is faced with a new attack mode, that is CCPAS (Coordinated Cyber-Physical AttackS). This kind of attack mode is not only hidden but also can cause chain failure, which is easy to cause large-scale power failure. Firstly, the basic forms of CPPS suffering CCPAS are described. CCPAS model considering state estimation constraint is constructed under the DC power flow model. Then, the mechanism of CCPAS is discussed, the maximum attack range after circumventing state estimation monitoring is analyzed from the attacker's point of view, and the vulnerable lines of CPPS are analyzed under CCPAS scenarios. Finally, taking IEEE 14- and 118-bus systems as the examples, the validity and applicability of the proposed model are verified through simulation and calculation, and the limitations of physical attack after considering the state estimation constraints are compared and analyzed.

Key words: smart grid; cyber-physical system; state estimation; coordinated cyber-physical attacks; false data injection attack

附　录

表 A1 各阶段的线路功率变化量

Table A1 Variation of line power at each stage

MW

线路	$\boldsymbol{P}_l^{(0)}$	本文模型			文献[22]		
		$\Delta\boldsymbol{P}_l^{(1)}$	$\boldsymbol{P}_l^{(3)}$	$\boldsymbol{P}_l^{(1)}$	$\Delta\boldsymbol{P}_l^{(1)}$	$\Delta\boldsymbol{P}_l^{(3)}$	$\boldsymbol{P}_l^{(1)}$
1−2	156.83	-75.56	156.83	81.27	-5.44	147.88	152.89
1−5	75.56	-48.4	75.56	—	5.44	71.12	66.11
2−3	73.18	-12.67	73.18	60.51	**-23.85**	**70.15**	**94.2**
2−4	56.13	-26.52	56.13	29.62	11.63	55.23	44.23
2−5	41.52	-36.38	41.52	5.15	8.83	40.9	32.77
3−4	-23.34	-12.67	-23.34	-36.01	**39.59**	**-24.15**	—
4−5	-61.14	-39.18	-61.14	**-100.33**	-12.22	-62.34	-49.89
6−11	7.26	0	7.26	7.26	0	6.3	29.43
6−12	9.0	0	9.0	9.0	0	7.55	16.89
6−13	16.69	0	16.69	16.69	0	17.03	41.38
7−8	0	0	0	0	0	0	5.88
7−9	28.03	0	28.03	28.03	0	28.99	7.48
9−10	5.32	0	5.32	5.32	0	6.2	16.81
12−13	2.81	0	2.81	2.81	0	1.45	0.00
13-14	5.8	0	5.8	5.80	0	4.98	29.43
14-9	-9.16	0	-9.16	-9.16	0	-9.92	6.62
10-11	-3.7	0	-3.7	-3.70	0	-2.8	10.2
4-7	28.03	0	28.03	28.03	0	28.99	-2.38
4-9	16.06	0	16.06	16.06	0	16.63	1.38
5-6	44.16	7.02	44.16	**51.18**	2.04	42.08	4.7

注：“—”表示相应线路断开。