DOI: 10.7667/PSPC180003

考虑负荷虚假数据注入攻击的电力信息物理系统防御策略

王电钢[1]，黄 林[1]，刘 捷[1]，吕 磊[1]，阮 振[2]，吕 林[2]

(1. 国网四川省电力公司信息通信公司，四川 成都 610041；2. 四川大学电气信息学院，四川 成都 610052)

摘要：为了更好地保障电网安全稳定运行，以电力信息物理高度融合为背景，结合博弈论思想，研究了电力信息物理系统攻防的具体过程，分析了一定防御资源下的最优防御方案及最小负荷期望损失。首先，以上层防御者制定最优防御方案降低电网脆弱性，中层攻击者制定最优防御策略最大化攻击效果，下层运行人员采取最优调度措施降低攻击损失为思路建立了一种三层优化模型。其次，基于遍历思想结合遗传算法和混合整数规划模型制定三层模型求解方案。最后基于算例分析，验证了该模型的有效性。

关键词：电力信息物理系统；防御策略；虚假数据注入攻击；攻防博弈

Cyber-physical system defense strategy considering loaded false data injection attacks

WANG Diangang[1], HUANG Lin[1], LIU Jie[1], LÜ Lei[1], RUAN Zhen[2], LÜ Lin[2]

(1. State Grid Sichuan Information and Communication Company, Chengdu 610041, China;
2. School of Electrical Engineering and Information, Sichuan University, Chengdu 610052, China)

Abstract: In order to achieve the higher security level of power system in context of cyber-physical fusion, the detailed procedures of attacks and defenses are studied in this paper based on the three-level framework of game theory. The optimal defense strategy and the minimal load loss expectation under the limited defense resources are also investigated. Firstly, the optimal defense strategy is modeled in the upper defender model to reduce the vulnerability of power grid. Then, the middle attacker model is established to maximize the attack effects. In the lower-level, the optimal dispatch is used to reduce the attack loss. To solve the problem efficiently, mixed integer programming method combined with traversal thought based genetic algorithm is employed to calculate the optimal results. The feasibility of the proposed approach is validated through a benchmark case study.

This work is supported by National Natural Science Foundation of China (No. 51437003).

Key words: cyber-physical system; defense strategy; false data injection attack; offensive and defensive game

0 引言

信息物理系统(Cyber Physical System, CPS)是计算进程和物理进程的统一体, 通过 3C(Computing、Communication、Control)技术的有机融合与深度协作，在环境感知的基础上实现大型工程动态控制[1-3]。近年来，随着智能电网的建设与发展，可再生能源、智能电表、智能传感器的大量接入，电力系统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，形成了具备CPS典型特征的电力CPS。电力 CPS 通过对电力系统全面详细的感知与分析，实现合理的动态控制，使封闭的电力系统向高度互联和信息共享的信息物理系统转化。然而传统电力系统设计之初，没有充分考虑到网络安全因素，因此物理系统与信息系统的深度融合，为电力系统带来了新的安全挑战[4-11]。目前，针对电网信息系统的网络攻击事件越来越频繁。典型的造成严重后果的是 2015 年乌克兰大停电事故[12]。近两年来，以色列电力局及纽约鲍曼水坝等也曾遭受过蓄意信息攻击[13-14]。

关于电力信息物理系统防御策略的研究受到各国学者的广泛关注。文献[15]对一种针对电力系统的协同攻击场景进行分析，并提出采用一种严格的二阶段求解方法以识别因攻击所造成的最大损失。

基金项目：国家自然科学基金项目资助(51437003)；国网四川省电力公司科技项目资助“信息系统数据状态与一次系统运行状态关联分析系统研究”

文献[16]讨论了攻击者利用不完全电网网络信息制定不可检测的协同攻击方案及防御策略。文献[17]考虑同步相量测量装置(Phasor Measurement Unit, PMU)的大量接入，如何通过不良数据检测装置检验虚假数据注入攻击。文献[18]以图论为基础，建立了电力 CPS 跨空间连锁故障危害评估模型。文献[19-20]利用博弈论思想分析了电网拒绝服务(Denial-of-service, DoS)攻击、虚假数据注入攻击与物理攻击协同作用时的最优防御方案。文献[21]以攻防博弈模型为基础，给出了电力 CPS 脆弱性评估方法及相应防御方案。文献[22]针对分层控制的电力 CPS 系统，提出了 CPS 建模和信息网络故障评估的方法。目前大多数学者对于针对电网的蓄意攻击研究中，更多的是将电力系统和信息系统分开单独研究，而充分考虑两者耦合关系的研究较少，且对于具体的攻击场景研究较少。

本文主要针对一种特殊的考虑虚假数据注入攻击的电力 CPS 协同攻击场景，提出最优防御方案规划模型。首先以动态攻防博弈思想为基础，建立三层博弈模型，之后针对具体攻击场景，给出每一层的具体目标函数和约束条件，并对该三层模型给出了具体的求解方案，最后以算例分析证明了该策略的有效性。

1　协同攻击场景

针对电力 CPS 的蓄意攻击按照攻击目的进行分类，大致可分为破坏性攻击和误导性攻击两种。破坏性攻击能够直接影响物理系统，造成负荷损失甚至网络崩溃。误导性攻击通过使控制系统及调度人员错误掌握电网信息，间接影响物理系统，获取经济利益或扩大电网损失。而配合良好的破坏性攻击和物理攻击将对电网造成更大的损失[23]。

充分的发电机和线路容量是电力系统正常运行的基础。发电机攻击和线路攻击是两种典型的能够给电网带来重大损失的破坏性攻击。同时，电力系统的稳定运行高度依赖调度人员通过对系统运行状态的实时监控而做出的调度决策。但是，实时监控的测量数据可能并不完全可靠，作为一种典型的误导性攻击，负荷虚假数据注入攻击能够通过入侵电网各节点的 SCADA 等量测采集系统，修改各节点负荷数据，使电网调度人员错误掌握电网负荷分配，从而在遭受攻击时做出错误的调度决策，造成更大的负荷削减甚至连锁故障。当不法分子掌握足够的物理及信息攻击资源时，能够对电力系统进行协同深度攻击，造成严重损失。接下来将对这种低频率高风险的攻击模型进行具体分析。

2　三层动态攻防博弈模型

随着现代科学的不断发展，研究的问题规模越来越大，结构越来越复杂，求解计算也越来越困难。Bracken 和 McGill 在 1973 年提出了二层规划模型，对分层递阶决策系统进行了初步讨论，上世纪 80 年代以后，随着博弈论的广泛应用，多层规划模型引起了众多学者的关注[24-25]。三层规划模型的一般形式为

$$\begin{cases} \max\limits_{x} \ f_1(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \\ \text{s.t.} \ g_1(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \le 0 \\ \max\limits_{y} \ f_1(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \\ \text{s.t.} \ g_2(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \le 0 \\ \max\limits_{z} \ f_1(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \\ \text{s.t.} \ g_3(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \le 0 \end{cases} \tag{1}$$

式中：$\boldsymbol{x} \in \boldsymbol{R}^{n1}$、$\boldsymbol{y} \in \boldsymbol{R}^{n2}$、$\boldsymbol{z} \in \boldsymbol{R}^{n3}$ 为每一层的决策变量；$f_i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$，$i = 1, 2, 3$ 分别为每一层的目标函数；而 $g_i(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}) \le 0$，$i = 1, 2, 3$ 则为每一层的约束条件。

其决策机制与双层决策模型类似，首先由上层确定其决策变量 $\boldsymbol{x}$ 的值，然后中层在相应 $\boldsymbol{x}$ 的取值下做出反应，确定其决策变量 $\boldsymbol{y}$ 的值，最后由下层在相应 $\boldsymbol{x}$、$\boldsymbol{y}$ 的取值下确定其决策变量 $\boldsymbol{z}$ 的取值。完成这一过程后，上层再根据中下层的决策调整自己的决策值，中下层又根据上层调整的决策值重新做出决策，如此循环达到整个系统的最优决策。

针对本文讨论的电力 CPS 具体协同攻防场景，第一步由防御者事先制定防御方案；第二步攻击者在知晓防御者的防御措施后，制定相应的信息物理协同攻击方案；第三步防御者在遭受协同攻击以后，采取相应的措施使电网负荷损失降到最低。即式(1)中，$\boldsymbol{x}$ 为防御者的防御资源分配向量，$\boldsymbol{y}$ 为攻击者攻击向量，$\boldsymbol{z}$ 为电网遭受协同攻击后防御者的最小负荷削减向量。具体的三层目标函数及约束条件如式(1)所示。

2.1　上层模型

电网防御者制定相应的防御措施及防御资源分配策略，将一定总量的防御资源分配到各条线路上，使得各条线路或发电机遭受物理攻击后被摧毁的概率降低，从而降低电网遭受协同攻击后的综合损失。分析上层模型，首先应对防御资源分配及攻击成功概率关系建模。对于第 m 个目标，令 DC_m 为降低该目标攻击成功率的最低攻击投资，当该目标攻击资源满足 $D_m \ge DC_m$ 时，攻击成功概率 $q_m(D_m)$ 为

$$q_m(D_m)=\mathrm{e}^{-\alpha_m D_m} \tag{2}$$

对于第 m 物理目标，D_m 为分配到该物理目标的防御资源，$\alpha_m=-\ln(q_{m0})/DC_m$，$DC_m$ 为最低投资，q_{m0} 为最低防御投资时的攻击成功率。当 $D_m \le DC_m$ 时，$p_m(A_m)=1$。实际电网规划中，防御资源有限。令防御资源总量为 D_{Total}，则有

$$\sum D_m \le D_{\text{Total}} \tag{3}$$

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。对于某一具体防御方案，令电网遭受攻击后综合损失为 $L=q_m\sum P_{\text{C},i}$，$P_{\text{C},i}$ 为 i 个节点的负荷损失。则上层目标函数为

$$\min \ \max\{q_m P_{\text{C}}\} \tag{4}$$

式中：q_m 为该防御方案的攻击成功概率，由式(2)计算；P_{C} 为该防御方案下，攻击者选择最优攻击方案且防御者在遭受攻击后采取最优应对措施下的负荷削减总量。具体计算方法由中下层模型给出。

2.2 中层模型

电网防御者制定相应的防御方案以后，攻击者根据电网的具体防御措施制定相应的最优攻击策略。本文假定攻击者完全掌握防御者防御资源分配信息，则中层目标函数为

$$\max \ q_m P_{\text{C}} \tag{5}$$

攻击策略采用负荷虚假数据注入攻击协同物理攻击的攻击方案。为使负荷虚假数据注入攻击成功不被检测，需满足各点负荷总和在攻击前后保持不变，且负荷变化量不得超过某一范围。即

$$\sum_{i=1}^{N_{\text{D}}}\Delta P_i=0 \tag{6}$$

$$-\tau P_i \le \Delta P_i \le \tau P_i \tag{7}$$

式中：ΔP_i 为第 i 个节点遭受虚假数据注入攻击后的测量有功负荷变化值；P_i 为第 i 个节点的原始有功功率负荷；τ 为基于历史运行数据确定的常量[8]，本文 τ 取 0.5。

2.3 下层模型

电网遭受协同攻击以后，通过调整发电机出力，启用备用机组等应对方案仍然不能满足负荷需求时，应及时采取负荷削减措施，以防止电网产生连锁故障，保证电网稳定运行。下层模型研究在上中层给出的攻防方案下，如何通过合理的负荷削减，使攻击造成的损失最小。即目标函数为

$$\min \ P \tag{8}$$

式中，P 为上中层的攻防方案下各节点负荷削减总和。满足如式(9)。

$$P=\sum_{i=1}^{N_{\text{D}}}P_{\text{C},i} \tag{9}$$

式中：$P_{\text{C},i}$ 为遭受攻击后，电网第 i 个节点的负荷损失；N_{D} 为系统总节点数。针对电力 CPS 的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误差不大，且方便计算，故本文采用直流潮流计算模型对 $P_{\text{C},i}$ 建模。即下层约束条件为

$$\text{s.t.} \ \sum_{i=1}^{N_{\text{D}}}P_{\text{SP},i}=0 \tag{10}$$

$$P_{\text{SP},i}=P_{\text{G},i}-(P_{\text{D},i}+\Delta P_{\text{D},i}-P_{\text{C},i})\ \forall i \tag{11}$$

$$\boldsymbol{F}=\boldsymbol{M}_{\text{f}}\times\boldsymbol{B}^{-1}\times\boldsymbol{P}_{\text{SP}} \tag{12}$$

$$-F_j^{\max}\le F_j\le F_j^{\max}\ \ j\in[1,N_{\text{F}}] \tag{13}$$

$$P_{\text{G},k}^{\min}\le P_{\text{G},k}\le P_{\text{G},k}^{\max}\ \ k\in[1,N_{\text{G}}] \tag{14}$$

$$0\le P_{\text{C},i}\le P_{\text{D},i}\ \forall i \tag{15}$$

$$P_{\text{G},k}^{\max}=P_{\text{G},k}^{\max}-\eta_k P_{\text{G},k}^{\max}\ \forall k \tag{16}$$

式中：$P_{\text{SP},i}$ 为第 i 个节点的注入功率；$P_{\text{G},i}$、$P_{\text{D},i}$ 分别描述第 i 个节点的发电机有功出力及有功负荷；$\Delta P_{\text{D},i}$ 为第 i 个节点的测量有功负荷变化值；$\boldsymbol{F}$ 为支路潮流向量；$\boldsymbol{M}_{\text{f}}$、$\boldsymbol{B}$ 分别为中层的攻击方案下电网的支路-节点关联的导纳矩阵和支路导纳矩阵。$\boldsymbol{P}_{\text{SP}}$ 为节点注入功率向量。式(13)为支路潮流约束，F_j 为第 j 条线路潮流；$F_j^{\max}$ 为该线路最大载流；N_{F} 为支路数。式(14)为发电机出力约束，$P_{\text{G},k}$ 为第 k 台机组有功出力；$P_{\text{G},k}^{\max}$、$P_{\text{G},k}^{\min}$ 分别为第 k 台机组出力上下限；N_{G} 为发电机数。式(15)表示节点的负荷削减不得大于该节点实际负荷。式(16)为物理攻击后发电机出力上限约束，η_k 为表征第 k 台机组是否遭受攻击的逻辑向量。

3 模型求解思路

目前对于非线性三层模型的求解暂无广泛适用的高效方法。针对本文的具体问题，三层模型直接求解效率极低且收敛性差。而由于电网攻击者攻击方案中，物理攻击目标数有限，则协同攻击中物理攻击方案的决策数有限，参考文献[21]及文献[26]的计算思路，在攻防双方都是理性人的前提下，攻击者能够选择最优的攻击方案，此时算出所有攻击方案的损失大小，通过防御资源分配降低所有方案

中的损失最大值，即可求得该攻防博弈的均衡解。即将第 2 节中三层模型转化为二阶段模型求解，第一阶段遍历所有的协同攻击方案，调用中下层优化函数，计算得到每种攻击方案的损失大小。第二阶段利用第一阶段的优化结果，考虑上层约束条件，求解得到最优的防御方案。求解步骤流程框图如图 1 所示。

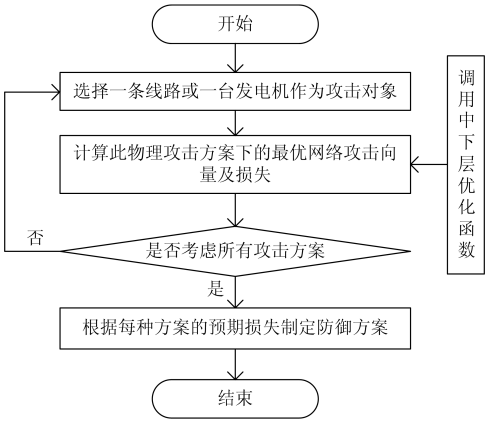

图 1 总优化求解流程图

Fig. 1 Total optimization algorithm flow chart

第一阶段中下层优化函数采用遗传算法求解，其求解步骤流程图如图 2 所示。下层为混合整数线性规划模型，利用 yalmap 平台快速求解。第二阶段利用文献[27]的计算方法，先确定防御资源精度，然后将有限的防御资源依次分配到遭受攻击后损失最大的几个目标上，使负荷损失的最大值减小，得到最优的防御方案。

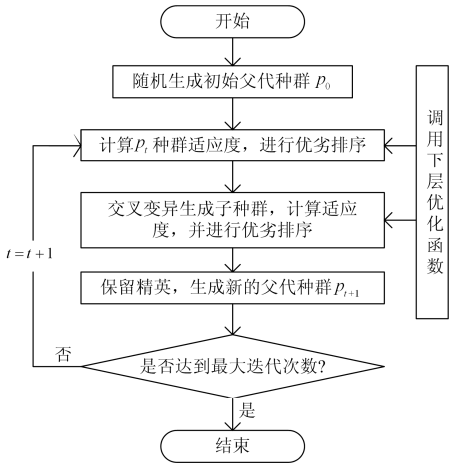

图 2 遗传算法优化求解流程图

Fig. 2 Flow chart of genetic algorithm optimal solution

4 算例分析

4.1 参数设置

本文基于修改的 IEEE5 机 14 节点系统作为研究对象，系统接线图如图 3 所示。

线路 1-2 的容量 $F^{\max}$ 参数设置为 160 MVA，线路 2-3 $F^{\max}$ 参数设置为 100 MVA，其他线路 $F^{\max}$ 参数设置为 30 MVA。其他参数由 Matpower 的 case14.m 文件中获取。发电机容量参数及防御投资参数如表 1 所示。各线路及发电机 DC 参数统一设置为 100，q_0 统一设置为 0.9。针对发电机、线路的总防御资源 D_{Total} 分别为 300、500、700 和 500、1 000、1 500。

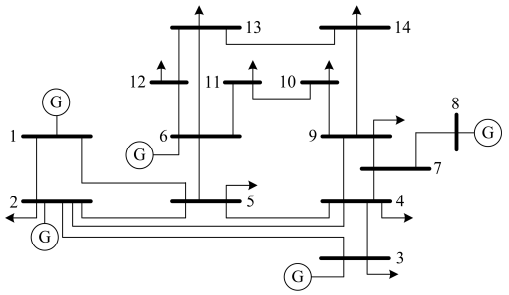

图 3 14 节点接线图

Fig. 3 14-bus system

表 1 发电机参数

Table 1 Generator parameter

机组编号	1	2	3	4	5
节点	1	2	3	6	8
最小有功出力/MW	0	0	0	0	0
最大有功出力/MW	200	50	30	50	20

4.2 优化结果

第一阶段，不考虑防御方案，针对每一种可能的攻击目标，由中下层模型求解出与物理攻击相配合的最佳网络攻击向量及有功负荷损失。以发电机和线路为目标的优化结果分别如表 2、表 3 所示。

表 2 发电机遭受攻击后仿真结果

Table 2 Generator attack simulation results

发电机编号	1	2	3	4	5
总负荷损失/MW	102.51	74.67	94.68	72.87	75.47

表 3 线路遭受攻击后仿真结果

Table 3 Transmission line attack simulation results

线路	总负荷损失/MW	线路	总负荷损失/MW
1-2	86.43	7-8	68.67
1-5	58.13	7-9	61.09
2-3	103.81	9-10	62.81
2-4	79.52	9-14	60.94
2-5	47.77	10-11	46.34
3-4	52.57	12-13	61.93
4-5	69.07	13-14	60.98
6-11	63.32	4-7	64.28
6-12	58.37	4-9	60.94
6-13	56.99	5-6	65.73

第二阶段，确定每台发电机或线路配合网络攻击有功损失后，以式(2)、式(3)为约束条件求解上层防御资源分配策略，使线路最大期望损失最小。发电机总防御资源为 300，线路总防御资源为 500 时，防御资源分配策略优化结果如表 4、表 5 所示。

表 4 发电机防御资源分配策略 $D_{\text{Total}}=300$

Table 4 Generator resource allocation strategy $D_{\text{Total}}=300$

发电机编号	防御资源	期望负荷损失/MW
1	187.71	84.12
2	0	74.67
3	112.29	84.12
4	0	72.87
5	0	75.47

表 5 线路防御资源分配策略 $D_{\text{Total}}=500$

Table 5 Transmission line defense resource allocation strategy $D_{\text{Total}}=500$

线路	防御资源	期望负荷损失/MW	线路	防御资源	期望负荷损失/MW
1-2	113.05	76.72	7-8	0	68.67
1-5	0	58.13	7-9	0	61.09
2-3	286.95	76.72	9-10	0	62.81
2-4	100	71.57	9-14	0	60.94
2-5	0	47.77	10-11	0	46.34
3-4	0	52.57	12-13	0	61.93
4-5	0	69.07	13-14	0	60.98
6-11	0	63.32	4-7	0	64.28
6-12	0	58.37	4-9	0	60.94
6-13	0	56.99	5-6	0	65.73

由表 4、表 5 可知，发电机总防御资源为 300 时，攻击者攻击发电机 1 或发电机 3，可造成电网最大负荷期望损失，为 84.12 MW。线路防御资源为 500 时，攻击者攻击线路 1-2 或 2-3，造成电网最大负荷期望损失，为 76.72 MW。负荷最大期望损失与防御资源的关系如图 4、图 5 所示。由图 4、图 5 可知，随着物理防御资源的增加，期望负荷损失逐渐减小。且期望负荷损失减小速率随着总防御资源的增多呈现下降趋势。

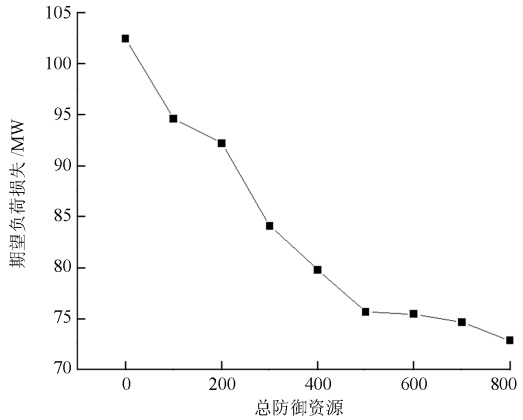

图 4 发电机攻击负荷损失曲线

Fig. 4 Load loss curve under generator attack

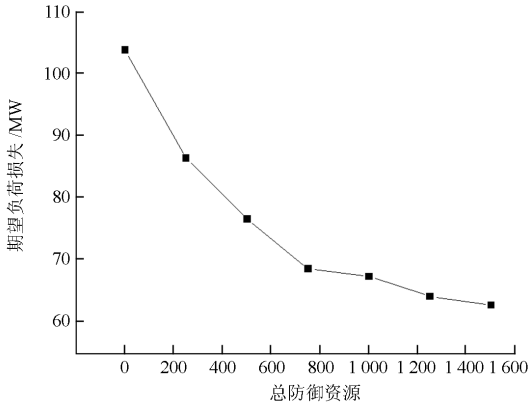

图 5 线路攻击负荷损失曲线

Fig. 5 Load loss curve under transmission line attack

5 总结

本文在电网信息层与物理层高度耦合的背景下，给出了考虑负荷数据虚假注入时信息物理协同攻击场景下的攻击威胁定量评估方法及最优防御资源分配策略。基于博弈论思想提出了三层优化模型并给出了求解方案，最后在算例分析中求解了不同防御资源下的最优防御方案及最小的期望负荷损失。

本文对电力 CPS 协同攻击防御策略的研究尚处于初步探索阶段，如非线性三层模型采用遍历求解方法，应用于大系统计算量仍较大。后续工作将进一步深化电力 CPS 协同攻击及防御方案的研究。

参考文献

[1] RAJKUMAR R, LEE I, SHA L, et al. Cyber-physical systems: the next computing revolution[C] // Design Automation Conference, June 13-18, 2010, Anaheim, CA, USA: 731-736.

[2] WOLF W. Cyber-physical systems[J]. Computer, 2009, 42(3): 88-89.

[3] 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.

[4] 黄良, 高正浩, 曹洪, 等. 一二次系统融合的电网风险评估实用化计算方法及数据建模研究[J]. 电力系统保护与控制, 2016, 44(17): 104-110.
HUANG Liang, GAO Zhenghao, CAO Hong, et al.

Research on calculation model for electric power system risk assessment with consideration of both primary and secondary system[J]. Power System Protection and Control, 2016, 44(17): 104-110.

[5] 伊洋, 刘育权, 陈宇强, 等. 基于信息综合判断的智能变电站网络通信故障定位技术研究[J]. 电力系统保护与控制, 2016, 44(3): 135-140.
YI Yang, LIU Yuquan, CHEN Yuqiang, et al. Research of network communication fault location technique in smart substation based on comprehensive information judgment[J]. Power System Protection and Control, 2016, 44(3): 135-140.

[6] 章熙, 王宏宇, 陈胜. 调度自动化系统运行监管信息模型建模研究[J]. 广东电力, 2017, 30(2): 110-115.
ZHANG Xi, WANG Hongyu, CHEN Sheng. Research on modeling for operating supervising information model of dispatching automation system[J]. Guangdong Electric Power, 2017, 30(2): 110-115.

[7] 陈锦山, 唐志军, 何燕玲, 等. 智能变电站二次系统信息安全测试方法[J]. 广东电力, 2017, 30(9): 75-80.
CHEN Jinshan, TANG Zhijun, HE Yanling, et al. Testing method for information security of secondary system of intelligent substation[J]. Guangdong Electric Power, 2017, 30(9): 75-80.

[8] 李霞, 李勇, 曹一家, 等. 基于信息物理系统融合的广域互联电网阻尼控制策略[J]. 电力系统保护与控制, 2017, 45(21): 35-42.
LI Xia, LI Yong, CAO Yijia, et al. Wide-area damping control strategy of interconnected power grid based on cyber physical system[J]. Power System Protection and Control, 2017, 45(21): 35-42.

[9] 李文武, 游文霞, 王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制, 2011, 39(10): 140-147.
LI Wenwu, YOU Wenxia, WANG Xianpei. Survey of cyber security research in power system[J]. Power System Protection and Control, 2011, 39(10): 140-147.

[10] 陈磊, 王永庆, 杨昊. 电网安全分析与仿真技术的现状分析及发展趋势研究[J]. 智慧电力, 2017, 45(8): 33-38.
CHEN Lei, WANG Yongqing, YANG Hao. Study on current situation and development trend of power grid security analysis and simulation technology[J]. Smart Power, 2017, 45(8): 33-38.

[11] 胡斌, 郭亚飞, 杨彬, 等. 智能变电站技术的现状与发展趋势研究[J]. 智慧电力, 2018, 46(3): 87-90.
HU Bin, GUO Yafei, YANG Bin, et al. Research on the current situation and decvelopment trend of smart substation technology[J]. Smart Power, 2018, 46(3): 87-90.

[12] 王得金. 从乌克兰电网被攻击事件看我国基础电网面临的安全风险及处置建议[J]. 中国信息安全, 2016(3): 91-93.

[13] 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. Cyber physical power systems: 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.

[14] 苏盛, 吴长江, 马钧, 等. 基于攻击方视角的电力 CPS 网络攻击模式分析[J]. 电网技术, 2014, 38(11): 3115-3120.
SU Sheng, WU Changjiang, MA Jun, et al. Attacker's perspective based analysis on cyber attack mode to cyber-physical system[J]. Power System Technology, 2014, 38(11): 3115-3120.

[15] LI Z, 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.

[16] LI Z, SHAHIDEHPOUR M, ABDULWHAB A, et al. Analyzing locally coordinated cyber-physical attacks for undetectable line outages[J]. IEEE Transactions on Smart Grid, 2018, 9(1): 35-47.

[17] DENG R, 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.

[18] 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.

[19] LI Y, SHI L, CHENG P, et al. Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach[J]. IEEE Transactions on Automatic Control, 2015, 60(10): 2831-2836.

[20] WEI L, SARWAT A, SAAD W, et al. Stochastic games for power grid protection against coordinated cyber-physical

attacks[J]. IEEE Transactions on Smart Grid, 2018, 9(2): 684-694.

[21] 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.

[22] LIU N, ZHANG J, ZHANG H, et al. Security assessment for communication networks of power control systems using attack graph and MCDM[J]. IEEE Transactions on Power Delivery, 2010, 25(3): 1492-1500.

[23] XIANG Y, WANG L, YU D, et al. Coordinated attacks against power grids: load redistribution attack coordinating with generator and line attacks[C] // Power & Energy Society General Meeting, July 26-30, 2015, Denver, CO, USA: 1-5.

[24] BRACKEN J, MCGILL J T. Mathematical programs with optimization problems in the constraints[J]. Operation Research, 1973(21): 37-44.

[25] STACKELBERG H. The theory of the market economy[M[. Oxford: Oxford University Press, 1952.

[26] 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. Assessment method of vulnerable communities in power grid considering cyber-physical integration[J]. Electric Power Automation Equipment, 2017, 37(12): 67-72, 79.

[27] CHEN G, DONG Z Y, HILL D J, et al. Exploring reliable strategies for defending power systems against targeted attacks[J]. IEEE Transactions on Power Systems, 2011, 26(3): 1000-1009.

收稿日期：2018-01-02； 修回日期：2018-05-17

作者简介：

王电钢(1973—)，男，博士，高级工程师，研究方向为电力信息物理融合系统。E-mail: 378453651@qq.com

(编辑 许 威)