

考虑电-气耦合系统连锁故障的多阶段信息物理协同攻击策略

曹茂森¹,王蕾报¹,胡博¹,谢开贵¹,伏坚¹,温力力²,
周平²,范璇²,李博²,曾意²

(1. 重庆大学 输配电装备及系统安全与新技术国家重点实验室,重庆 400044;
2. 国网重庆市电力公司经济技术研究院,重庆 401120)

摘要:针对电-气耦合系统在恶意攻击下的风险分析,提出了一种计及电-气耦合系统连锁故障的信息物理多阶段协同攻击策略。为了诱导调度人员做出错误调度决策和降低电网的安全裕度,提出了一种以最大化线路过载程度为目标的改进负荷重分配(LR)攻击模型。综合考虑天然气系统与电力系统的调度时间尺度差异,构建一种新型的电-气耦合系统多阶段协同攻击策略:初始阶段通过攻击气网侧气源或管道以影响电-气耦合节点的天然气机组状态,然后针对电力系统交替采用改进LR攻击和物理攻击,最终导致大规模连锁停运。基于Q-Learning提出了最优策略求解算法,以比利时20节点天然气系统和IEEE 30节点系统为算例,验证了所提信息物理协同攻击模型的正确性和有效性。

关键词:多能源系统;电-气耦合系统;负荷重分配攻击;信息物理协同攻击;连锁故障;Q-Learning 算法

中图分类号:TP 393;TM 71

文献标志码:A

DOI:10.16081/j.epae.201908041

0 引言

近年来,随着煤炭等传统能源的日益匮乏,而社会经济发展对能源的需求不断增大,多能源综合利用技术受到了越来越高的关注^[1]。相较于风、光等可再生能源的间歇性和波动性,天然气可以同时为天然气网和电力网持续地供能。对于电力系统的可靠性与电能质量的影响而言,天然气发电是一种更可靠和稳定的发电方式^[2]。由于其具有清洁、高效率、高质量等特性,天然气已经成为一些地区的主要供应能源。

在多能源系统紧密耦合提升能源效率的同时,不同能源系统之间的交互影响也可能给电力网带来运行风险^[3]。在多能源系统中,单个能源网络内部的故障可能诱发其他能源系统的连锁反应。2004年6月29日,新加坡由于天然气供应中断而造成大面积停电,22个地区内的30万户居民和企业受到影响。此外,在“8·15”台湾大停电事件中,由于操作人员失误,导致6台天然气机组全部跳闸,从而引起全岛连锁停电。因此为了保证多能源系统的安全运行,分析天然气网与电力网络之间故障的交互影响具有重要意义。

现有研究已经针对电-气耦合系统建立了较为详细的物理和数学模型,同时基于电-气耦合模型提出一系列的多能源系统联合优化算法^[4]。文献[5]

提出一种考虑多能源网络、多类型储能和风电相关性的多能源系统随机日前调度模型,以减少风电的削减,提高多能源系统运行灵活性。文献[6]从可持续发展的角度出发,结合现有能源利用和其他清洁能源,着重研究多能源系统的经济性,分析电-气多能源系统的联合运行成本和运行结构优化。文献[7]以不确定性区间刻画可再生能源和电力需求的不确定性,研究了满足多能源需求下并网微电网容量规划的多目标优化方法。同时,为了评估多能源系统的可靠性水平,文献[8]考虑多能源系统负荷和元件故障的不确定性,提出电-气耦合系统的可靠性评估方法,分析结果表明接入一定容量的电转气装置可有效减少系统“弃风限电”现象,提高系统可靠性。而文献[9]的研究则表明在峰荷阶段,随着电-气耦合程度的提高,天然气系统中的随机故障将显著增加电力系统连锁故障的风险。

作为多能源系统联合运行和电力系统安全监控的核心支撑技术,信息物理系统(CPS)高度融合的智能电网是实施新能源战略的重要平台,在调整我国能源结构、节能减排方面具有宏大意义^[10]。借助于电力信息物理系统中的分布式传感器实时获知电网数据^[11],运行人员可及时调整电网运行状态以保证供电安全。但随着智能电网中信息技术的大规模应用,电力信息物理系统也成为了恶意攻击的新对象。2015年乌克兰大停电事故即由电网信息系统遭受黑客恶意攻击导致,该事故对当地22.5万人的正常生活造成了严重影响^[12]。因此在智能电网中,恶意攻击已经成为造成系统大停电不可忽视的诱因

收稿日期:2019-04-08;修回日期:2019-07-05

基金项目:国家自然科学基金资助项目(51725701)

Project supported by the National Natural Science Foundation of China(51725701)

之一。

在现有研究中,电力系统可能遭受的恶意攻击主要考虑3类事件。第一类是以物理系统为目标的物理攻击。文献[13-14]提出了基于连锁故障网络图的输电线路脆弱性评估方法,研究线路攻击与线路故障传播的时序关系。文献[15]考虑了线路攻击的时间特性,通过2层优化模型确定线路攻击的最佳位置和最佳攻击时间。第二类是针对信息系统的网络攻击。该部分大多数研究着眼于刻画负荷重分配(LR)攻击对系统可靠性的影响,即建立基于直流潮流的LR攻击双层优化模型^[16],通过LR攻击使得电力系统损失较多负荷甚至诱发连锁故障^[17]。第三类则是针对信息物理系统的协同攻击。文献[18]提出了一种同时计及LR攻击、机组攻击和线路攻击的双层协同攻击模型。文献[19]研究结果表明,采用信息物理协同攻击方式会比独立攻击产生更严重的后果。但是,上述所有文献的研究均侧重于在电力系统范畴内分析攻击后果,而鲜有涉及对电-气耦合的多能源系统风险分析。事实上,天然气系统的突发故障和运行调整也会对电力系统的安全可靠运行产生重大影响。因此,研究电-气耦合下的信息物理协同攻击风险对多能源系统建设有重要意义。

本文基于攻击者视角,研究了在电-气耦合背景下,同时考虑连锁故障和LR的信息物理系统多阶段协同攻击策略。首先,通过分析电力系统与天然气系统的时间尺度差异,建立了针对天然气系统和电力系统的协同攻击方式;然后在此基础上,以诱发电力系统侧的连锁故障为目标,提出了一种结合LR攻击和线路攻击的信息物理协同攻击模型;最后,提出了一种基于Q-Learning的最优攻击策略求解算法。以比利时20节点天然气系统和IEEE 30节点电力系统为算例,分析电-气耦合系统下信息物理协同攻击所带来的停电风险,为多能源系统安全运行提供参考。

1 电-气耦合系统

电-气耦合系统是指天然气网和电力网组成的多能源互联系统,其典型结构如附录中图A1所示。天然气网主要元件包括管道、气源、储气设施和压缩机等。压缩机的主要功能是弥补在传输过程中由于损耗而降低的气压,保持管道气压在正常范围内。电力系统的主要元件包括发电机组、输电线路、变压器等。在本文所考虑的电-气耦合系统模型中,天然气机组作为电-气系统交互的主要设备,因此特别地将天然气机组所在节点等效形成电-气耦合节点。天然气机组通过电-气耦合节点连接管道将注入的天然气转化为电能供给电力系统负荷。

1.1 天然气网运行优化模型

1.1.1 目标函数

本文中天然气网运行状态由最小成本优化模型确定,即:

$$\min \sum_{m=1}^N \tau_{m,G} S_m + \tau_{m,LC} \Delta S_m \quad (1)$$

其中, N 为天然气网的总节点数; S_m 和 ΔS_m 分别为节点 m 处气源供应量和天然气削负荷量; $\tau_{m,G}$ 和 $\tau_{m,LC}$ 分别为节点 m 处供应成本和削负荷成本系数。

1.1.2 管道流量约束

天然气管道流量主要由管道两端气压及管道长度等参数决定。

对于不含压缩机的管道,天然气只能从高压节点向低气压节点流动,关系式如下:

$$\text{sgn}(p_m, p_n) f_{mn}^2 = M_{mn} (p_m^2 - p_n^2) \quad (2)$$

$$\text{sgn}(p_m, p_n) = \begin{cases} 1 & p_m > p_n \\ -1 & p_m < p_n \end{cases} \quad (3)$$

$$p_{m,\min} \leq p_m \leq p_{m,\max} \quad (4)$$

$$f_{mn,\min} \leq f_{mn} \leq f_{mn,\max} \quad (5)$$

其中, f_{mn} 和 p_m, p_n 分别为通过管道 mn 的流量和管道 mn 两端的气压; $\text{sgn}(p_m, p_n), M_{mn}$ 分别为管道 mn 流量的流向、管道流量系数; $p_{m,\max}, p_{m,\min}$ 分别为节点 m 气压的上、下限; $f_{mn,\max}, f_{mn,\min}$ 分别为管道 mn 流量的上、下限。

对于含有压缩机的管道,天然气从低气压节点向高压节点流动,通过压缩机的流量可表示为:

$$\text{sgn}(p_m, p_n) f_{mn}^{\text{cp}} = (p_m^2 - p_n^2) \frac{H_{mn}}{k_2 - k_1 \left(\frac{\max(p_m, p_n)}{\min(p_m, p_n)} \right)^{\alpha_1}} \quad (6)$$

$$H_{mn,\min} \leq H_{mn} \leq H_{mn,\max} \quad (7)$$

其中, f_{mn}^{cp} 为含压缩机管道的流量; k_1, k_2, α_1 为与压缩机有关的经验系数; H_{mn} 和 $H_{mn,\max}, H_{mn,\min}$ 分别为管道 mn 上压缩机的输入功率和输入功率的上、下限。

压缩机运行时需要在吸气侧(低压侧)消耗额外的天然气驱动其汽轮机,可表示为:

$$\tau_{mn}^{\text{cp}} = a_c H_{mn}^2 + b_c H_{mn} + c_c \quad (8)$$

其中, τ_{mn}^{cp} 为压缩机运行时消耗的天然气; a_c, b_c 和 c_c 为压缩机消耗系数。

此外,由于压缩机特性的影响,压缩机的升压比例需保持在一定范围内:

$$R_{mn,\min} \leq \frac{p_m}{p_n} \leq R_{mn,\max} \quad (9)$$

其中, $R_{mn,\max}, R_{mn,\min}$ 分别为管道 mn 上压缩机的升压比例上、下限。

由于管道流量式(2)和式(6)为非线性约束,一

般需采取分段线性化方法进行近似处理,将模型转化为混合整数线性规划求解^[20]。

1.1.3 节点流量平衡约束

对于天然气网中的每个节点,天然气流入量和流出量相等,可表示为:

$$S_m - (S_{m,L} - \Delta S_m) = \sum_{n=1}^M f_{mn} + \sum_{n=1}^{N_{CP}} f_{mn}^{cp} + \sum_{n=1}^{N_{CP}} \tau_{mn}^{cp} \quad (10)$$

$$S_{m,\min} \leq S_m \leq S_{m,\max} \quad (11)$$

$$0 \leq \Delta S_m \leq S_{m,L} \quad (12)$$

其中, $S_{m,L}$ 为节点 m 处天然气原始负荷; M 、 N_{CP} 分别为天然气网的管道数量、压缩机数量; $S_{m,\max}$ 、 $S_{m,\min}$ 分别为节点 m 气源出气量的上、下限。

此外,当确定天然气网各节点的负荷削减量后,可通过电-气耦合节点更新天然气机组的出力:

$$P_{mi,g} = \eta (S_{m,L} - \Delta S_m) \quad (13)$$

其中, η 为天然气机组的转化效率; $P_{mi,g}$ 为与天然气网节点 m 相耦合的电网节点 i 天然气机组输出功率。

1.2 电力网潮流模型

直流潮流属于线性模型,求解复杂度明显低于非线性的交流潮流,在OPA、隐故障等连锁故障模拟模型中广泛采用^[21]。因此,本文采用直流潮流进行潮流计算,其模型表示为:

$$F_l = \frac{1}{X_l} \sum_{b=1}^{N_B} A_{bl} \theta_b \quad l=1,2,\dots,N_L \quad (14)$$

其中, F_l 为线路 l 流过的有功潮流; X_l 为线路 l 的电抗; A_{bl} 为节点-线路关联矩阵的第 b 行第 l 列的元素; θ_b 为节点 b 的相角; N_B 、 N_L 分别为电网中节点总数、线路总数。

2 信息物理攻击简介

2.1 信息攻击

信息攻击是指在电力信息物理系统中通过入侵信息系统对运行数据或者控制信号进行篡改干扰的行为。其中,较常见的一种攻击形式是LR攻击,具体而言是指攻击人员通过恶意修改电力系统中的负荷测量数据以误导运行人员的调度行为,进而使得系统遭受较大损失的一种攻击形式。

现有的LR攻击模型通常采用基于直流潮流的双层模型来描述,如式(15)~(24)所示。

$$\max \sum_{g=1}^{N_G} (a_g P_g^2 + b_g P_g + c_g) + \sum_{d=1}^{N_D} c_d S_d \quad (15)$$

$$\text{s.t.} \quad \sum_{d=1}^{N_D} \Delta L_d = 0 \quad (16)$$

$$-\tau L_d \leq \Delta L_d \leq \tau L_d \quad d=1,2,\dots,N_D \quad (17)$$

$$\min \sum_{g=1}^{N_G} (a_g P_g^2 + b_g P_g + c_g) + \sum_{d=1}^{N_D} c_d S_d \quad (18)$$

$$\text{s.t.} \quad \theta_r = 0 \quad (19)$$

$$F_l = \frac{1}{X_l} \sum_{b=1}^{N_B} A_{bl} \theta_b \quad l=1,2,\dots,N_L \quad (20)$$

$$\sum_{g=1}^{N_G} \Gamma_{bg} P_g = \sum_{d=1}^{N_D} D_{bd} (L_d + \Delta L_d - S_d) + \sum_{l=1}^{N_L} A_{bl} F_l \quad b=1,2,\dots,N_B \quad (21)$$

$$0 \leq S_d \leq L_d + \Delta L_d \quad d=1,2,\dots,N_D \quad (22)$$

$$-F_l^{\max} \leq F_l \leq F_l^{\max} \quad l=1,2,\dots,N_L \quad (23)$$

$$P_g^{\min} \leq P_g \leq P_g^{\max} \quad g=1,2,\dots,N_G \quad (24)$$

其中, ΔL_d 为节点 d 负荷测量值遭受LR攻击后的修改量; τ 为避免攻击被识别而限制的篡改幅度; a_g 、 b_g 和 c_g 为机组 g 的发电成本系数; c_d 为负荷点 d 的削负荷成本系数; N_G 和 N_D 分别为电网中机组总数和负荷节点总数; θ_r 为电力系统遭受信息攻击后参考节点的虚假相角; L_d 和 S_d 分别为负荷点 d 的负荷和负荷削减量; P_g 为机组 g 的有功出力; Γ_{bg} 为节点-机组关联矩阵的第 b 行第 g 列的元素; D_{bd} 为节点-负荷关联矩阵的第 b 行第 d 列的元素。

在该双层攻击模型中,上层模型式(15)~(17)定义了攻击者策略。攻击者的目标是(15)是最大限度地增加系统运行成本,运行成本包括发电成本和削负荷成本。约束式(16)表明所有负荷节点负荷测量值的修改量代数和为0,目的是保证系统的供需平衡。约束式(17)限制了LR攻击中负荷测量值的篡改幅度,使攻击行为不会被运行人员发现。下层模型式(18)~(24)模拟了电力系统在遭受LR攻击后的优化调度过程,目标函数是系统的发电成本和负荷削减成本最小。在式(19)中将参考节点的相角设为0。式(20)和式(21)保证系统中每个节点的功率平衡,式(22)~(24)分别为削负荷量、线路潮流和机组出力范围约束。

由于目标函数式(15)仅考虑单次LR攻击造成的负荷损失最大,导致攻击者只关注于眼前利益。而对于以诱发系统大停电为目标的攻击者而言,单次的信息攻击或者物理攻击并不一定能导致系统发生大规模停电,因此,攻击者需要进行多次的攻击行为,即多阶段攻击模式,这将在3.2节具体介绍。

当一条线路发生随机故障或者受到物理攻击而退出运行时,该线路的原有功率在系统剩余线路上重新分配,即潮流转移。如果潮流转移使某些线路处于过负荷状态,会导致线路温度上升,并且随着线路潮流越过热稳定极限的程度加深,线路停运概率逐渐增大^[22]。因此,不同于现有模型,本文将LR攻击的目标函数改进为式(25),即攻击者的目标是诱导调度人员做出错误的运行决策,使得在物理攻击之前最大化线路过载程度。同时为了分析线路的实际过载状态,在上层模型中添加约束式(26)~(28)。

$$\max \sum_{l=1}^{N_L} \frac{|F_l^A|}{F_l^{\max}} \quad (25)$$

$$F_l^A = \frac{1}{X_l} \sum_{b=1}^{N_B} A_{bl} \theta_b^A \quad l=1,2,\dots,N_L \quad (26)$$

$$\theta_r^A = 0 \quad (27)$$

$$\sum_{g=1}^{N_G} \Gamma_{bg} P_g = \sum_{d=1}^{N_B} D_{bd} (L_d - S_d) + \sum_{l=1}^{N_L} A_{bl} F_l^A \quad b=1,2,\dots,N_B \quad (28)$$

其中, F_l^A 为线路 l 的真实潮流; θ_b^A 为节点 b 的真实相角; θ_r^A 为电力系统遭受信息攻击后参考节点的真实相角。式(26)~(28)为系统遭受 LR 攻击后的线路真实潮流约束,其中机组出力 P 和负荷削减量 S 为下层模型的决策变量。综上,式(16)~(28)为本文所提的考虑连锁故障影响的改进 LR 信息攻击模型。该双层模型可以通过 KKT 方法转化为单层混合整数线性规划问题进行求解^[23]。

2.2 物理攻击

物理攻击是指针对电-气耦合系统物理实体设备的攻击,而攻击成功会导致该设备故障停运。对于攻击者,输电线路和天然气管道是所有物理攻击对象中最容易攻击的目标,因为它们通常具有较大的地理跨度,难以监控^[19]。此外,由于天然气需求快速增长,气源供应紧张,为简化表征,本文考虑的物理攻击对象为气网中的气源、天然气管道和电力网络中的输电线路。它们被攻击成功的影响后果分别如下。

气源 m 被攻击后将不能正常运行,该气源出气量为 0,如式(29)所示。

$$\tilde{S}_m = 0 \quad (29)$$

其中,“~”为被攻击的标志。

天然气管道 mn 被攻击后会使得该管道的流量为 0,如式(30)所示。

$$\tilde{f}_{mn} = 0 \quad (30)$$

输电线路 l 被攻击后会停运,则对应线路的潮流为 0,如式(31)所示。

$$\tilde{F}_l = 0 \quad (31)$$

3 多能源系统的信息物理协同攻击策略

当天然气网遭受物理攻击破坏时,可能导致部分天然气负荷被切除,影响电网侧天然气机组出力。此外,相较于单阶段攻击模式,多阶段信息物理协同攻击通过信息攻击干扰电网运行人员的调度决策,间接改变电网运行状态,配合物理攻击诱发电网连锁故障,造成大规模的线路故障和负荷损失。综上,本文提出如附录中图 A2 所示的计及电-气耦合的多阶段信息物理协同攻击策略。本文假设攻击者能获得实时系统拓扑结构和设备参数等数据,并对测控

系统具有一定的恶意控制能力^[24]。

3.1 天然气系统攻击模型

在电力系统中电能以光速进行传播,即电网运行功率状态保持实时同步更新。相较而言,天然气在管道中的流动则是一个非常缓慢的物理过程,导致天然气系统的运行时间尺度明显高于电力系统^[25]。气网侧在遭受攻击后经历较长时间才会达到新的稳态并对电网侧产生影响。综上,本文主要考虑对天然气系统进行最优的单阶段物理攻击,即假设攻击者仅在初始阶段对气网侧的多个设备进行物理攻击,并在气网侧达到新的稳态运行点后再对电网侧进行攻击。其目的是为了改变电-气耦合点的运行状态,进而影响电力系统侧的运行安全裕度。

3.2 计及电-气耦合的多阶段信息物理协同攻击策略

当天然气网在经历物理攻击后到达新稳态运行时,电力网随之同步进行运行状态更新。考虑到电力系统运行调度的即时性,攻击者可能采用多阶段攻击的形式达到诱发大停电的目的,并且在不同的阶段通过协调信息攻击和物理攻击造成更恶劣的影响,具体模拟过程如下。

(1)气网侧攻击模拟:选定气网侧的某些气源或管道作为攻击目标,更新对应元件的运行状态,同时根据式(1)~(12)模拟气网优化调度过程。

(2)更新电-气耦合节点状态:根据气网侧在遭受攻击后达到的新稳定点更新电力网中的电-气耦合节点状态,由式(13)确定电-气耦合节点处的天然气机组出力。

(3)信息攻击模拟:为了诱导系统运行人员进行错误的调度决策,攻击者依据改进 LR 模型进行信息攻击。在求解式(16)~(28)后,更新对应机组出力 and 负荷等系统运行状态。

(4)电网侧物理攻击:考虑到攻击资源的限制和电力系统的实时监控特性,本文在每个阶段的电网侧攻击中仅考虑攻击 1 条输电线路。

(5)电网连锁故障模拟。

a. 孤岛识别及功率平衡模拟:分析当前系统拓扑。若由于出现孤岛导致孤岛内供需功率不平衡,系统通过自动发电控制和低频减载装置自动平衡孤岛内的机组出力 and 负荷需求^[17]。由于天然气机组出力由天然气网优化调度确定^[9],孤岛内部调整平衡策略可分为以下 2 种。①如果火电机组与天然气机组出力之和低于负荷,火电机组首先根据其可用剩余出力按比例增大其出力;如果最大机组出力之和仍低于负荷,则按功率缺额比例依次削减负荷。②如果火电机组与天然气机组出力之和大于负荷,火电机组应先按比例下调出力以匹配负荷;如果最小机组出力之和仍大于负荷,则按容量大小由小到大

依次关停火电机组。

b. 线路连锁故障模拟:采用直流潮流模型更新各个孤岛潮流。由于线路潮流过载可能引起保护设备的动作,从而造成输电线路的连锁故障^[21]。本文采用概率模型模拟线路连锁故障:

$$p = \begin{cases} p_0 & F_{\text{line}} \leq F_{\text{line}}^{\max} \\ p_0 + \frac{F_{\text{line}} - F_{\text{line}}^{\max}}{1.4F_{\text{line}} - F_{\text{line}}^{\max}} (1-p_0) & F_{\text{line}}^{\max} < F_{\text{line}} < 1.4F_{\text{line}}^{\max} \\ 1 & F_{\text{line}} \geq 1.4F_{\text{line}}^{\max} \end{cases} \quad (32)$$

其中, p_0 为随机故障概率; F_{line} 、 F_{line}^{\max} 分别为线路当前功率、额定功率。

如果出现新的线路故障,则返回步骤**a**,否则转至步骤**c**。

c. 电网再调度模拟:在电网故障模拟过程终止时,根据最优切负荷模型模拟系统运行方调度行为。

(6)攻击终止判定:为了量化攻击对系统的影响,攻击过程的终止目标通常设定为特定的线路故障数或负载损失量阈值。若已达到攻击目标,协同攻击模型终止模拟,否则返回步骤(3)执行下一阶段电网侧的攻击。计及电-气耦合的多阶段信息物理协同攻击策略如附录中图A3所示。

4 基于Q-Learning的最优攻击算法

本文提出的信息物理协同攻击模型是一个典型的多阶段规划问题,而动态规划则是求解多阶段优化问题的主要算法之一。动态规划将复杂问题分成若干阶段逐段求解,从而确定全局最优解,但同时随着维数增加,计算量呈指数增长。针对该“维度灾”问题,本文采用强化学习(又称近似动态规划)中的Q-Learning算法求解多阶段最优攻击策略。强化学习的核心思想是智能体通过反馈学习获取环境最大奖励,逐步建立最优策略^[26]。其中包括3个核心参数:状态 D 、动作 X 和奖励 R 。针对多阶段攻击问题,本文依次做出如下的定义。

状态 D 表示每个阶段开始时系统所处的自然状况或客观条件。本文中状态 D 由天然气网气源、管道和电力网中线路的可用状态 D^{gas} 和 D^{elec} 组成,其中 $D^{\text{gas}} = [D_{g1}, D_{g2}, \dots, D_{gM}]$,其下标为天然气网中气源和管道序列号; $D^{\text{elec}} = [D_{e1}, D_{e2}, \dots, D_{eN_L}]$,其下标为电网线路序列号。

动作 X 表示决策体针对当前状态所采用的策略。本文中动作 X 包含对天然气网侧的物理攻击 X^{gas} 和对电网侧的信息攻击 X^{cyber} 与物理攻击 X^{elec} 。天然气网侧物理攻击 $X^{\text{gas}} = [X_{g1}, X_{g2}, \dots, X_{gM}]$,其中 X_{gi} 为对天然气网气源或管道 i 执行物理攻击;电网侧信息攻击 $X^{\text{cyber}} = [\Delta L_{d1}, \Delta L_{d2}, \dots, \Delta L_{dN_L}]$,其中 ΔL_{di}

为对电网节点 i 负荷执行恶意数据篡改;电网侧物理攻击 $X^{\text{elec}} = [X_{e1}, X_{e2}, \dots, X_{eN_L}]$,其中 X_{ei} 为对电力线路 i 执行物理攻击。

在强化学习过程中,状态 D 、物理攻击 X^{gas} 和 X^{elec} 由一系列二进制变量表示。信息攻击策略 X^{cyber} 由连续变量表示,可通过本文提出的LR攻击模型直接求解。

奖励 $R(D, X)$ 表示当前状态 D 下采用指定动作 X 后获得价值的期望值。对于本文电网侧每阶段的物理攻击 X^{elec} ,定义环境奖励 $R(D, X)$ 如下:

$$R(D, X) = \frac{n_{\text{cas}}}{N_{\text{object}}} \quad (33)$$

其中, n_{cas} 为由当前阶段协同攻击引起的电网线路故障数; N_{object} 为恶意攻击者希望通过整个多阶段攻击最终实现的故障线路总数。

对于气网侧的物理攻击 X^{gas} ,由于无法直接量化其对电网侧的攻击效果,本文在实现总的电网侧攻击目标后,再由式(34)确定气网物理攻击 X^{gas} 的奖励值。

$$R(D, X) = \begin{cases} \frac{N_{\text{object}}}{n_{\text{stage}}} & n_{\text{stage}} < N_{\text{object}} \\ -1 & n_{\text{stage}} = N_{\text{object}} \end{cases} \quad (34)$$

其中, n_{stage} 为本轮训练中为实现攻击目标所进行的攻击阶段数目。式(34)表示所用攻击阶段数越少,则该攻击策略 X^{gas} 越有效。

根据Bellman方程,为表征在某一状态 D 中采取不同动作 X 后带来的后期收益期望,强化学习通过状态动作值 $Q(D, X)$ 评估不同的状态-动作组合 (D, X) 。且由Bellman方程可知 $Q(D, X)$ 满足^[27]:

$$Q(D, X) = R(D, X) + \gamma \max_{X'} Q(D', X') \quad (35)$$

其中, D' 为在当前状态 D 中执行动作 X 后的下一个系统状态; γ 为折算系数,为保证收敛一般取值略小于1。

由于电网连锁故障模拟是一个随机过程,式(33)和式(34)的奖励 $R(D, X)$ 同样为不确定函数。为改善算法收敛性,采用迭代更新策略如下:

$$Q(D, X) = (1-\alpha)Q(D, X) + \alpha [R(D, X) + \gamma \max_{X'} Q(D', X')] \quad (36)$$

其中, α 为学习率,在训练开始时设置为0.9,并随着训练次数的增加逐渐降低。

在此基础上,根据 $1-\varepsilon$ 原则选择状态 D 中的最优动作:

$$X = \begin{cases} \arg \max Q(D, X) & 1-P_{\text{exploration}} \\ \text{random} & P_{\text{exploration}} \end{cases} \quad (37)$$

其中, $P_{\text{exploration}}$ 为强化学习过程中随机选择攻击目标的概率。可以在保证学习历史经验能力的同时避免陷入局部最优解。应用Q-Learning确定最优协同攻

击策略的算法流程如附录中图 A4 所示。

5 算例分析

本文以比利时 20 节点天然气系统^[28]和 IEEE 30 节点电力系统组成的电-气耦合系统为算例,结构图如附录中图 A5 所示。在本文中,物理攻击考虑的对象为气网中的气源、天然气管道和电力网络中的输电线路,即附录图 A5 中红色标注元件。在 3.2 GHz Core-i5 6500 CPU 和 8 G RAM 的台式计算机上,采用 MATLAB 2018a 对所提的协同攻击策略进行求解,其中改进 LR 模型采用 YALMIP 工具箱^[29]调用 Gurobi 求解。

5.1 多阶段协同攻击策略效果分析

为了说明电-气耦合对所提的多阶段信息物理协同攻击策略的影响,本文采用以下 4 种场景进行分析:场景 1 为初始阶段不计及气网侧攻击;场景 2 为初始阶段选取气网侧 1 个元件进行攻击;场景 3 为初始阶段选取气网侧 3 个元件进行攻击;场景 4 为初始阶段选取气网侧 5 个元件进行攻击。

气网侧攻击元件包括天然气管道和气源。4 种场景下攻击目标均为导致电网侧任意 10 条线路故障停运,确定电-气耦合系统在协同攻击下的薄弱环节。此外,本文将 Q-Learning 算法中训练次数均设置为 1 500。设所有状态-动作组合的 $Q(D, X)$ 初始值为 1, α 和 γ 分别为 0.9 和 0.1, $P_{\text{exploration}}$ 初始值为 1, 且随训练次数衰减,最低为 0.1。

附录中图 A6 比较了 4 种场景下完成攻击目标的收敛曲线,实验结果为 3 次重复试验的平均值。从图中可见,在 4 种场景下,攻击次数均随着训练次数的增加而减少,证明本文所提的 Q-Learning 算法使攻击有效性得到持续提升。表 1 给出了在不同场景下算法收敛后,为实现攻击目标,最优攻击方案下电网侧信息物理协同攻击的平均次数。结果表明相较于未计及气网侧故障影响(场景 1)的电网侧攻击,计及气网侧故障影响(场景 2—4)的电网侧攻击均具有更高的有效性。而且随着气网侧攻击资源的增加,电网侧所需攻击的平均次数进一步降低。这是由于在场景 2—4 初始阶段,气网侧攻击会导致部分电-气耦合点的天然气机组出力下降。为满足负荷需求,其余火电机组出力上升,引起电网部分区域

表 1 最优攻击策略的平均攻击次数对比

Table 1 Comparison of average attack times under optimal attack strategies

协同攻击 场景	气网侧攻击 元件数	平均攻击次数 (电网侧)
1	0	4.74
2	1	4.14
3	3	2.53
4	5	1.88

的线路负载过高。一旦重载线路受到攻击后潮流大规模转移可能引起更多的线路连锁故障。除此之外,随着气网最大攻击资源数量的增多,电-气耦合点受到的影响程度愈加变大,电网侧受到气网侧故障的风险传播影响更为严重,更易诱发连锁故障。

同时注意到,附录图 A6 中的攻击效果最终会在一定的水平范围内波动,而不是稳定收敛在某一定值上。这是由于本文采用了式(32)所示的隐故障模型,电力系统的连锁故障属于随机过程。且式(37)始终保证存在随机选择攻击目标的可能,也会导致攻击效果有小概率波动。

5.2 最优攻击策略分析

为更好地体现本文模型的特征,以场景 1 与场景 3 为例进行详细说明。本小节将对表 2 所示的最优攻击策略进行详细分析。表中,符号[]内的线路表示由于上条线路停运后引发的连锁停运线路,若符号[]内为空则表示上条线路停运后未引发新的连锁故障;箭头表示诱发后续线路退出运行,如场景 3 第一攻击阶段中“6-9→[6-8]”表示线路 6-9 停运后诱发线路 6-8 退出运行。从表中可知,场景 3 中气网攻击阶段仅针对管道 14-15、15-16 和 4-14 执行物理攻击,而并未对气源执行攻击,这说明在当前场景下天然气管道被攻击对电力系统的影响大于气源被攻击对电力系统的影响。电网侧攻击第一阶段在执行 LR 信息攻击后,对线路 6-9 执行了物理攻击,该攻击依次诱发了线路 6-8 等 5 条线路退出运行。而第二阶段在执行 LR 信息攻击后,对线路 2-6 进行物理攻击,随后依次诱发线路 2-4 等 8 条线路故障。同时从表 2 可见,场景 1 下最优攻击策略需要经过 4 次攻击电网线路后才能实现攻击目标。

表 2 最优攻击策略对比

Table 2 Comparison of optimal attack strategies

攻击模式	最优攻击策略	
	场景 1	场景 3
气网侧攻击阶段	—	14-15, 15-16, 4-14
电网侧攻击 第一阶段	2-5→[]	6-9→[6-8]→[8-28]→ [9-10, 9-11]→[4-12]
电网侧攻击 第二阶段	4-6→[2-6, 5-7, 4-12]	2-6→[2-4, 6-10]→[1-3, 3-4, 24-25, 25-27, 28-27, 6-28]
电网侧攻击 第三阶段	12-13→[9-11, 6-8, 8-28]	—
电网侧攻击 第四阶段	15-18→[]	—

表 3 为场景 3 第一阶段 LR 攻击前、后的机组出力变化,表 4 为场景 3 第一阶段连锁故障线路开断前、后(括号内数值)负载率变化。在场景 3 的初始阶段,3 条气网管道 14-15、15-16 和 4-14 故障导致流过管道 14-15 和 15-16 的天然气体量为 0。由式(13)可知,节点 16 实际天然气体荷量等于 0,即供给

电-气耦合点中天然气机组 G_6 的天然气为 0, 天然气机组 G_6 输出功率也为 0 (原始出力为 28.80 MW), 故该机组退出运行, 迫使位于电网北部的火电机组出力增加。然而由于该系统负荷主要分布于南部 (G_6 为南部主要电源之一), 系统潮流分布更加不均匀, 9-10 和 9-11 等线路明显重载。而且由表 3 可见, 在经历电网侧第一阶段的 LR 攻击后, 机组 G_2 出力由 61.15 MW 调低至 26.89 MW, 机组 G_4 出力由 61.15 MW 上升到 97.20 MW, 造成系统潮流分布进一步恶化。从表 4 可见, 在线路 6-9 受到物理攻击停运时, 线路 6-8 的负载率从 0.59 增加至 1.37, 这是由于保护动作被切除。由于线路 6-8 故障后潮流转移, 线路 8-28 的负载率上升至 1.68, 同样被保护切除。进一步同时诱发线路 9-10 和 9-11 过载停运。最终, 第一阶段在线路 4-12 停运后进入新的稳态, 此时电网已经解列成为 4 个孤岛。在第二阶段中由于孤岛内机组较少, LR 攻击未产生影响。但通过线路 2-6 物理攻击后, 同样引起线路 2-4 等 8 条线路先后过载, 造成连锁停运。此时系统已解列为多个孤岛, 连锁故障停止。攻击共造成电网侧 15 条线路停运, 目标达成。

表 3 LR 攻击前、后的机组出力变化
Table 3 Variation of generator output before and after LR attack

节点	机组出力 / MW	
	攻击前	攻击后
1	54.75	54.75
2	61.15	26.89
5	45.20	45.20
8	61.15	97.20
11	61.15	59.36
13	0	0
合计	283.40	283.40

表 4 连锁故障线路开断前、后负载率变化
Table 4 Variation of load ratio before and after disconnection of cascading failure lines

连锁故障过程	当前故障线路	连锁故障线路	开断前、后连锁故障线路负载率变化
1	6-9	6-8	0.59(1.37)
2	6-8	8-28	0.31(1.68)
3	8-28	9-11, 9-10	0.95(1.46), 0.97(1.48)
4	9-11, 9-10	4-12	0.28(1.23)

6 结论

本文提出了一种考虑电-气耦合和连锁故障的信息物理协同攻击策略, 为信息物理融合下的智能电网提供了新的停电风险分析途径。首先, 初始阶段选定气网侧的某些气源或管道作为攻击目标, 以影响电-气耦合节点状态; 然后, 对电网侧进行多阶段攻击, 具体包括通过信息攻击诱导系统运行人员做出错误的调度决策, 降低系统运行的安全裕度, 进

一步通过实施物理攻击诱发连锁故障, 最终导致大规模连锁停运; 最后, 采用 Q-Learning 算法分析了最优攻击策略。

算例结果表明由于电-气耦合系统中不同运营方调度的独立性, 在天然气网受到攻击导致故障后, 电网侧可能受到风险传播影响, 导致电网潮流分布过于集中, 部分线路易出现过载, 更易诱发连锁故障。因此, 如何协同电-气耦合系统在故障下的联合调度以确保双方安全运行, 是下一步亟需开展的工作。

附录见本刊网络版 (<http://www.epae.cn>)。

参考文献:

- [1] 邵成成, 王锡凡, 王秀丽, 等. 多能源系统分析规划初探[J]. 中国电机工程学报, 2016, 36(14): 3817-3828.
SHAO Chengcheng, WANG Xifan, WANG Xiuli, et al. Probe into analysis and planning of multi-energy systems[J]. Proceedings of the CSEE, 2016, 36(14): 3817-3828.
- [2] 田世明, 栾文鹏, 张东霞, 等. 能源互联网技术形态与关键技术[J]. 中国电机工程学报, 2015, 35(14): 3482-3494.
TIAN Shiming, LUAN Wenpeng, ZHANG Dongxia, et al. Technical forms and key technologies on energy internet[J]. Proceedings of the CSEE, 2015, 35(14): 3482-3494.
- [3] 骆柏锋, 穆云飞, 赵波, 等. 基于统一潮流模型的电-气耦合综合能源系统静态灵敏度分析[J]. 电力系统自动化, 2018, 42(13): 29-35.
LUO Baifeng, MU Yunfei, ZHAO Bo, et al. Static sensitivity analysis of integrated electricity and gas system based on unified power flow model[J]. Automation of Electric Power Systems, 2018, 42(13): 29-35.
- [4] SÁNCHEZ-MARTÍN P, CORREA-POSADA C M. Integrated power and natural gas model for energy adequacy in short-term operation[J]. IEEE Transactions on Power Systems, 2015, 30(6): 3347-3355.
- [5] ZHANG Rufeng, JIANG Tao, LI Guoqing, et al. Day-ahead scheduling of multi-carrier energy systems with multi-type energy storages and wind power[J]. CSEE Journal of Power and Energy Systems, 2018, 4(3): 283-292.
- [6] WANG Zhilong, WANG Zesen, CAO Jun, et al. Analysis on economic operation of multi-energy flow system[J]. The Journal of Engineering, 2017, 2017(13): 1494-1498.
- [7] LIU Zifa, WANG Xuyang, ZHUO Ranqun, et al. Flexible network planning of autonomy microgrid[J]. IET Renewable Power Generation, 2018, 12(16): 1931-1940.
- [8] 余娟, 马梦楠, 郭林, 等. 含电转气的电-气互联系统可靠性评估[J]. 中国电机工程学报, 2018, 38(3): 708-715.
YU Juan, MA Mengnan, GUO Lin, et al. Reliability evaluation of integrated electrical and natural-gas system with power-to-gas[J]. Proceedings of the CSEE, 2018, 38(3): 708-715.
- [9] 包铭磊, 杨阳, 丁一, 等. 考虑天然气系统影响的电力系统连锁故障评估[J]. 电网技术, 2019, 43(1): 1-9.
BAO Minglei, YANG Yang, DING Yi, et al. Assessment of cascading failures in power system considering effects of natural

- gas system[J]. Power System Technology, 2019, 43(1):1-9.
- [10] 鞠平,周孝信,陈维江,等. “智能电网+”研究综述[J]. 电力自动化设备, 2018, 38(5):2-11.
JU Ping, ZHOU Xiaoxin, CHEN Weijiang, et al. “Smart grid plus” research overview[J]. Electric Power Automation Equipment, 2018, 38(5):2-11.
- [11] 汤奕,王琦,倪明,等. 电力信息物理融合系统中的网络攻击分析[J]. 电力系统自动化, 2016, 40(6):148-151.
TANG Yi, WANG Qi, NI Ming, et al. Analysis of cyber attacks in cyber physical power system[J]. Automation of Electric Power Systems, 2016, 40(6):148-151.
- [12] SULLIVAN J E, KAMENSKY D. How cyber-attacks in Ukraine show the vulnerability of the US Power Grid[J]. The Electricity Journal, 2017, 30(3):30-35.
- [13] 韦晓广,高仕斌,李多,等. 基于连锁故障网络图和不同攻击方式的输电线路脆弱性分析[J]. 中国电机工程学报, 2018, 38(2):465-474, 677.
WEI Xiaoguang, GAO Shibin, LI Duo, et al. Cascading fault graph for the analysis of transmission network vulnerability under different attacks[J]. Proceedings of the CSEE, 2018, 38(2):465-474, 677.
- [14] 张国华,张建华,杨京燕,等. 基于有向权重图和复杂网络理论的大型电力系统脆弱性评估[J]. 电力自动化设备, 2009, 29(4):21-26.
ZHANG Guohua, ZHANG Jianhua, YANG Jingyan, et al. Vulnerability assessment of bulk power grid based on weighted directional graph and complex network theory[J]. Electric Power Automation Equipment, 2009, 29(4):21-26.
- [15] SAYYADI S, YOUSEFI G R, LATIFY M A. Mid-term vulnerability analysis of power systems under intentional attacks[J]. IET Generation, Transmission and Distribution, 2016, 10(15):3745-3755.
- [16] YUAN Yanling, LI Zuyi, REN Kui. Modeling load redistribution attacks in power systems[J]. IEEE Transactions on Smart Grid, 2011, 2(2):382-390.
- [17] CHE Liang, LIU Xuan, LI Zuyi, et al. False data injection attacks induced sequential outages in power systems[J]. IEEE Transactions on Power Systems, 2019, 34(2):1513-1523.
- [18] 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.
- [19] XIANG Yingmeng, WANG Lingfeng, LIU Nian. Coordinated attacks on electric power systems in a cyber-physical environment[J]. Electric Power Systems Research, 2017, 149:156-168.
- [20] SHAO Chengcheng, WANG Xifan, MOHAMMAD S, et al. An MILP-based optimal power flow in multicarrier energy systems[J]. IEEE Transactions on Sustainable Energy, 2017, 8(1):239-248.
- [21] CARRERAS B A, LYNCH V E, DOBSON I, et al. Complex dynamics of blackouts in power transmission systems[J]. Chaos, 2004, 14(3):643-652.
- [22] 程林,何剑,孙元章. 线路实时可靠性模型参数对电网运行可靠性评估的影响[J]. 电网技术, 2006, 30(13):8-13.
CHENG Lin, HE Jian, SUN Yuanzhang. Impact of transmission line's real-time reliability model parameter upon power system operational reliability evaluation[J]. Power System Technology, 2006, 30(13):8-13.
- [23] 张儒峰,姜涛,李国庆,等. 考虑电转气消纳风电的电-气综合能源系统双层优化调度[J]. 中国电机工程学报, 2018, 38(19):5668-5678.
ZHANG Rufeng, JIANG Tao, LI Guoqing, et al. Bi-level optimization dispatch of integrated electricity-natural gas system considering P2G for wind power accommodation[J]. Proceedings of the CSEE, 2018, 38(19):5668-5678.
- [24] 王琦,李梦雅,汤奕,等. 电力信息物理系统网络攻击与防御研究综述:(一)建模与评估[J]. 电力系统自动化, 2019, 43(9):9-21.
WANG Qi, LI Mengya, TANG Yi, et al. A review on research of cyber-attacks and defense in cyber physical power systems part one modeling and evaluation[J]. Automation of Electric Power Systems, 2019, 43(9):9-21.
- [25] LIU Cong, MOHAMMAD S, WANG Jianhui. Coordinated scheduling of electricity and natural gas infrastructures with a transient model for natural gas flow[J]. Chaos: An Interdisciplinary Journal of Nonlinear Science, 2011, 21(2):25102.
- [26] TSITSIKLIS J N. Asynchronous stochastic approximation and Q-learning[C]//Proceedings of the 32nd IEEE Conference on Decision and Control. San Antonio, TX, USA: IEEE, 1993:395-400.
- [27] 莫顿·I·凯曼,南茜·L·施瓦茨. 动态优化:经济学和管理学中的变分法和最优控制[M]. 2版. 北京:中国人民大学出版社, 2016:222-226.
- [28] WOLF D D, SMEERS Y. The gas transmission problem solved by an extension of the simplex algorithm[J]. Management Science, 2000, 46(11):1454-1465.
- [29] LOFBERG J. YALMIP: a toolbox for modeling and optimization in MATLAB[C]//IEEE International Conference on Robotics and Automation. New Orleans, LA, USA: IEEE, 2004:284-289.

作者简介:



曹茂森

曹茂森(1996—),男,四川资中人,硕士研究生,主要研究方向为电力系统运行分析与计算(**E-mail**: caomaosen@foxmail.com);

王蕾报(1993—),男,河北邢台人,博士研究生,主要研究方向为电力系统可靠性(**E-mail**: leibaowang1993@163.com);

胡博(1983—),男,河南南阳人,教授,博士,通信作者,主要研究方向为电力系统规划与可靠性、电力系统分析计算、并行计算(**E-mail**: hboy8361@163.com);

谢开贵(1972—),男,四川眉山人,教授,博士,主要研究方向为电力系统规划与可靠性、电力系统优化运行(**E-mail**: kaiguixie@vip.163.com);

伏坚(1995—),男,四川巴中人,硕士研究生,主要研究方向为电力系统规划与可靠性(**E-mail**: fujian@cqu.edu.cn)。

Coordinated cyber-physical multi-stage attack strategy considering cascading failure of integrated electricity-natural gas system

CAO Maosen¹, WANG Leibao¹, HU Bo¹, XIE Kaigui¹, FU Jian¹, WEN Lili²,
ZHOU Ping², FAN Xuan², LI Bo², ZENG Yi²

(1. State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University, Chongqing 400044, China; 2. State Grid Chongqing Economic Research Institute, Chongqing 401120, China)

Abstract: As for the risk analysis of integrated electricity-natural gas system under malicious attack, the coordinated cyber-physical multi-stage attack strategy that takes into account the cascading failure of integrated electricity-natural gas system is proposed. Firstly, in order to mislead the operator and reduce the safety margin of power grid, an improved LR (Load Redistribution) attack model is proposed to maximize the degree of line overload. Secondly, considering the time-scale difference of dispatching between natural gas system and power system, a new coordinated multi-stage attack strategy for integrated electricity-natural gas system is constructed. In the initial stage, gas sources or pipelines in gas system are attacked to influence the state of natural gas generators at the integrated electricity-natural gas node. Then, the improved LR attack and physical attack are adopted alternately to the power system, which eventually leads to a black-out. Finally, a Q-Learning based algorithm is proposed to identify the optimal attack strategy. The correctness and validity of the proposed attack strategy are verified by the Belgium 20-node natural gas system and the IEEE 30-bus system.

Key words: multi-energy system; integrated electricity-natural gas system; load redistribution attack model; coordinated cyber-physical attack; cascading failure; Q-Learning algorithm

(上接第127页 continued from page 127)

Multi-index evaluation for integrated energy system operation connecting transmission and distribution levels

HE Yubin^{1,2}, ZHANG Yining¹, MA Guang¹, GUO Chuangxin¹, ZHOU Yuyong³, YE Gangjin³

(1. College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China;
2. Power Dispatching and Control Center of China Southern Power Grid, Guangzhou 510623, China;
3. State Grid Hangzhou Power Supply Company, Hangzhou 310000, China)

Abstract: In order to quantify the impact of multiple uncertainties such as wind power fluctuations and equipment random failures on the IES (Integrated Energy System), a multi-index evaluation method for IES operation is proposed. In terms of modeling, the unified framework including the energy network in upper transmission level and the EH (Energy Hub) in lower distribution level is established, and the coupling characteristics of electricity, gas and heat in the whole process of generation-transmission-distribution-utilization are described in detail. In terms of methodology, wind power fluctuations and equipment failures are handled by state-space partitioning respectively, while the MS-MC (Mixed Scatter-Monte Carlo) sampling method is proposed to accelerate evaluation convergence. Meanwhile, sequential linearization method is adopted to solve the optimal multi-energy flow problem for the balance of approximation accuracy and solution speed, which further improves the efficiency of evaluation. In terms of indicators, facing the low carbon operation environment, a multi-index evaluation framework including operation economy, system reliability, wind power accommodation, environment protection and so on is established to comprehensively describe the impact of multiple uncertainties on IES operation. The effectiveness and rationality of the proposed methods are verified by the simulations on RTS79-40Node IES with 17 EHs.

Key words: integrated energy system; energy hub; energy management; reliability analysis; MS-MC sampling; sequential linearization; optimal multi-energy flow

附录

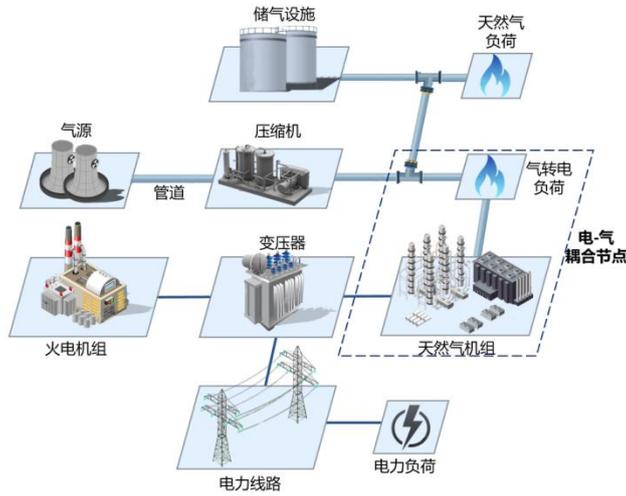
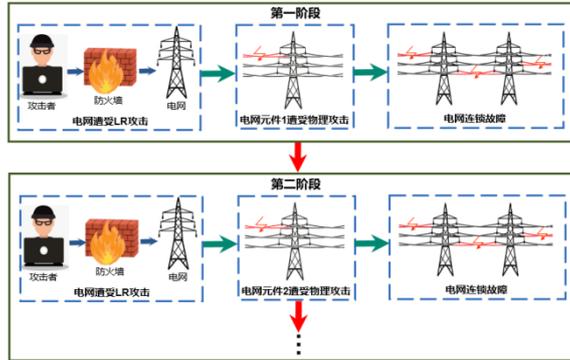


图 A1 电-气耦合系统示意图

Fig.A1 Schematic diagram of integrated electricity-natural gas system



(a) 电-气系统的协同攻击



(b) 电力系统的信息物理协同攻击

图 A2 电-气耦合系统的信息物理协同攻击框架

Fig.A2 Framework of coordinated cyber-physical attack for the integrated electricity-natural gas system

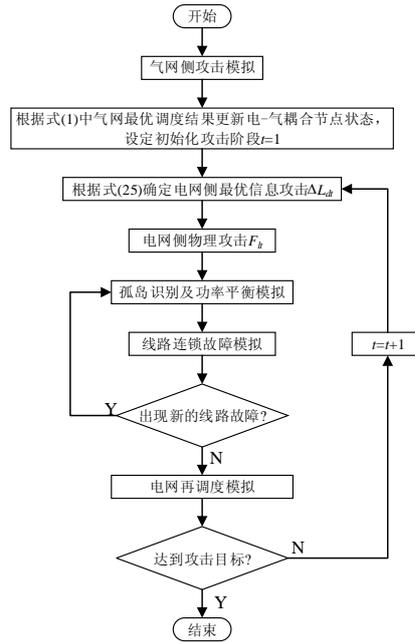


图 A3 计及电-气耦合的多阶段信息-物理协同攻击策略

Fig.A3 Coordinated cyber-physical multi-stage attack strategy of integrated electricity-natural gas system

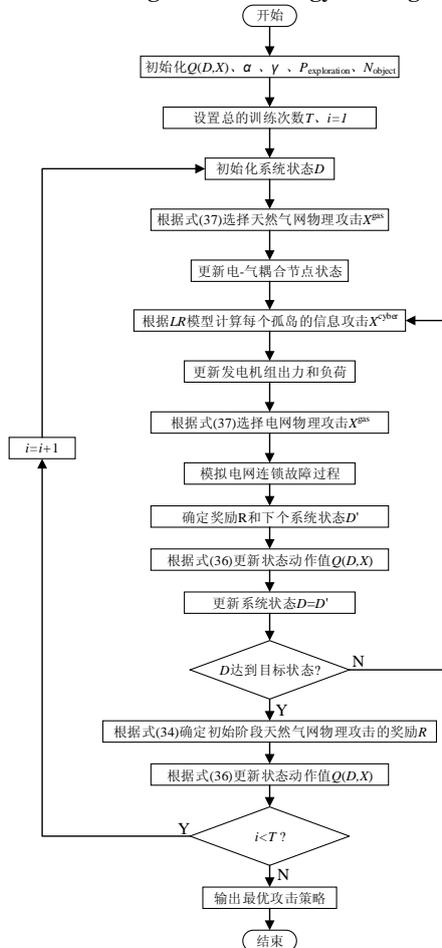


图 A4 基于 Q-learning 的最优攻击算法

Fig.A4 Q-learning based optimal attack algorithm

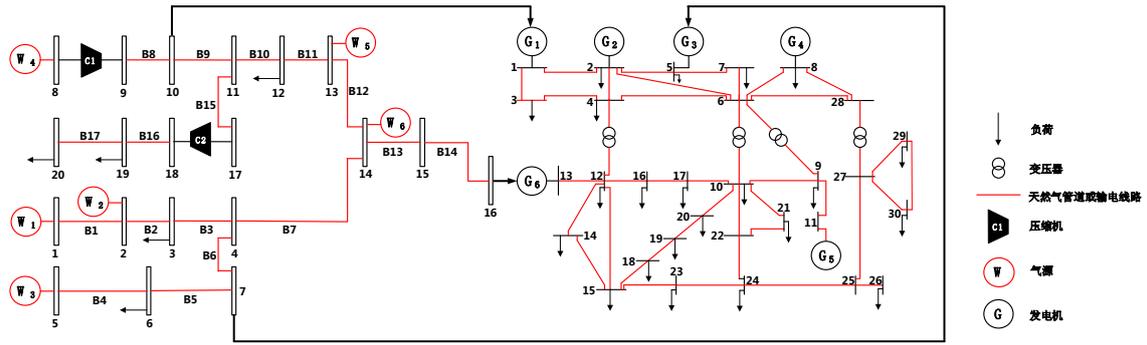
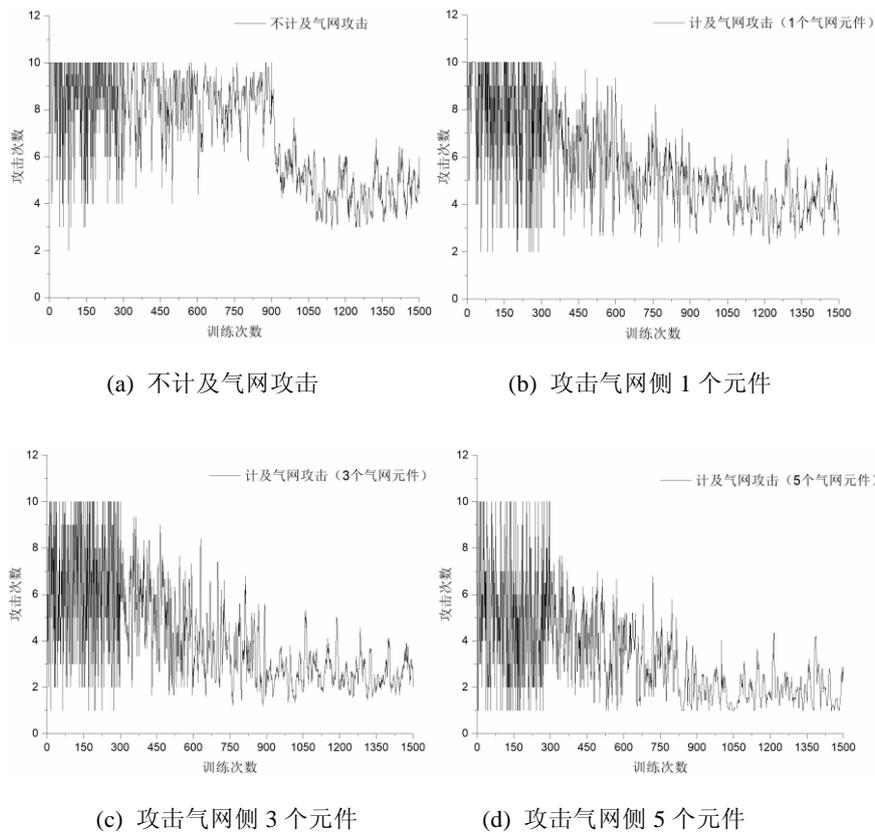


图 A5 电-气耦合系统结构图

Fig.A5 Structure of integrated electricity-natural gas system



(a) 不计及气网攻击

(b) 攻击气网侧 1 个元件

(c) 攻击气网侧 3 个元件

(d) 攻击气网侧 5 个元件

图 A6 基于 Q-learning 的攻击算法收敛曲线

Fig.A6 Convergence curve of Q-learning based attack algorithm