•新型电力系统•

DOI:10.15961/j.jsuese.202200310

本刊网刊

负荷重分配攻击下电–气系统损失评估与脆弱性分析

周步祥[1,2], 闵昕玮[1,2], 臧天磊[1,2*], 张远洪[1,2], 陈　阳[1,2], 赵雯雯[1,2]

(1.四川大学 电气工程学院, 四川 成都 610065; 2.智能电网四川省重点实验室(四川大学), 四川 成都 610065)

摘　要: 在电力信息物理系统中, 负荷重分配(load redistribution, LR)攻击是一种常见的虚假数据注入攻击。而在天然气网与电网耦合紧密的背景下, 针对电–气耦合系统(integrated electricity natural gas system, IEGS)的负荷重分配攻击可能会对系统的安全运行造成更严重的影响。因此本文对电–气耦合下的LR攻击展开深入研究。首先, 在分析IEGS双侧协同LR攻击作用机理的基础上, 研究LR攻击的实施策略。其次, 计及连锁故障对电网的影响, 以IEGS经济损失最大为目标函数, 建立IEGS下LR攻击的损失评估模型, 统一度量了不同能源子系统的损失, 量化了不同场景下LR攻击对系统安全经济运行的风险, 定义了新的节点综合脆弱性评价指标, 全面深层次分析IEGS中的高脆弱性节点。再次, 对天然气管道流量方程中的非线性项进行线性化处理, 将IEGS调度模型转化并添加到攻击者模型中, 作为Karush–Kuhn–Tucher(KKT)最优条件, 从而将整个模型转换为混合整数线性规划问题。最后, 在IEEE 39节点和改进比利时20节点算例系统上, 进行了3种LR攻击场景的仿真, 验证了3种攻击在不同攻击资源下的攻击效果, 分析了系统高脆弱性节点的分布与变化, 并给出了针对不同LR攻击形式的系统综合保护策略。实验结果表明, 双侧协同LR攻击会对系统造成更严重的损失, 但依据本文评估和分析方法采取综合保护策略后, 系统损失显著降低。

关键词: 电–气耦合系统; 双侧协同负荷重分配攻击; 节点脆弱性转移; 连锁故障

中图分类号: TM731　　**文献标志码**: A　　**文章编号**: 2096-3246(2023)01-0003-11

Loss Assessment and Vulnerability Analysis of an Integrated Electricity Natural Gas System Under Load Redistribution Attack

ZHOU Buxiang[1,2], *MIN Xinwei*[1,2], *ZANG Tianlei*[1,2*], *ZHANG Yuanhong*[1,2], *CHEN Yang*[1,2], *ZHAO Wenwen*[1,2]

(1.College of Electrical Eng., Sichuan Univ., Chengdu 610065, China;
2.Key Lab. of Intelligent Electric Power Grid in Sichuan Province (Sichuan Univ.), Chengdu 610065, China)

Abstract: Load redistribution (LR) attacks are common false data injection attacks in cyber-physical power systems. Under the background of close coupling between a natural gas network and a power system, the LR attack on the integrated electricity natural gas system (IEGS) may have a more serious impact on the safe operation of the system. Therefore, LR attacks were deeply studied under IEGS in this paper. First, based on the analysis of the mechanism of bilateral coordinated LR attack under IEGS, the implementation strategy of LR attack was studied. Second, considering the impact of cascading failures on the power system and taking the maximum economic loss of the IEGS as the objective function, the loss assessment model of LR attacks under IEGS was established. Meanwhile, the losses of different energy subsystems were measured uniformly, the risks of LR attacks on system security and economic operation under different scenarios were quantified, a new node comprehensive vulnerability evaluation index were defined, and the high vulnerability nodes in the IEGS were assessed comprehensively. Third, the nonlinear constraints in the natural gas pipe flow were linearized. The IEGS scheduling model was converted and added into the attack model as Karush–Kuhn–Tucher (KKT) optimality conditions, thus the whole model is transformed into a mix-integer linear programming. Finally, three LR attack scenarios were

收稿日期:2022 – 04 – 11

基金项目:国家自然科学基金项目(51907097); 四川省科技计划项目(2020JDRC0049)

作者简介:周步祥(1965—), 男, 教授, 博士生导师, 博士. 研究方向: 调度自动化、综合能源新技术. E-mail: hiway_scu@126.com

* **通信作者**:臧天磊, 副研究员, E-mail: zangtianlei@126.com

网络出版时间:2022 – 08 – 26 11 : 13 : 47　　**网络出版地址**:https://kns.cnki.net/kcms/detail/51.1773.tb.20220825.1656.001.html

simulated on the IEEE 39-bus and the improved Belgium 20-bus system. During the simulation process, the attack effects of the three attacks under different attack resources were verified. Besides, the distribution and change of high vulnerability nodes of the system were analyzed, and the comprehensive protection strategies for different LR attacks were proposed. The experimental results showed that the system suffered more serious losses under bilateral coordinated LR attack. However, after adopting the comprehensive protection strategy based on the evaluation and analysis methods proposed in this paper, the system loss is significantly reduced.

Key words: integrated electricity natural gas system; bilateral coordinated LR attack; node vulnerability transfer; cascading failure

智能电网作为典型的信息物理系统[1],承担了推动建设新型电力系统的重要任务。然而,信息物理的高度融合也使系统的安全风险急剧增加。2015年,乌克兰电网遭受信息攻击,造成其全国大面积停电,停电持续时间之长,影响范围之大,十分罕见[2]。由此可见,信息攻击引发的安全事件会造成严重的经济损失和恶劣的社会影响。同时,伴随着燃气发电技术的快速发展,电网与天然气网耦合程度不断加深[3]。天然气网和电网具有很强的相互依存性,针对天然气网的信息攻击会影响电网的安全运行[4]。因此,全面研究信息攻击机理与影响对电–气耦合系统(integrated electricity natural gas system, IEGS)安全稳定运行意义重大。

现有研究中,针对电力系统的信息攻击主要有以下两大类。第1类是信息–物理协同攻击,通过物理方法破坏电网中元件的同时发动信息攻击,以掩盖电网的真实运行状态,对电网造成严重的损失。田猛等[5]以攻击者和调度中心的目标冲突为基础建立双层规划模型,并针对电网中的脆弱性节点进行分析。伏坚等[6]提出防御性随机规划模型来应对协同攻击带来的风险。阮振等[7]建立了以电力系统最大化损失为目标的双层模型,并给出了节点在信息攻击下的脆弱性分析。以上研究虽然为保护系统信息安全提供了有效的支撑,但并不能直观反映信息攻击对于系统造成的损失,同时也未对系统内节点的脆弱性进行全面的评估,故不能真正反映系统内的高脆弱性节点。此外,协同攻击需要物理攻击的时效性较高,因此在实际中难以对电力系统实施信息物理协同攻击。第2类是单一信息攻击,在实际电力系统的攻击中较为常见。本文主要对信息攻击中的虚假数据注入攻击展开深入研究。虚假数据注入攻击可分为拓扑攻击和负荷重分配攻击(load redistribution, LR)。拓扑攻击通过篡改线路开断数据,误导调度中心的状态感知,危害系统安全。王超超等[8]建立了电力信息物理系统分层模型,考虑了多层耦合的特性,并基于拓扑分析方法对攻击进行了模拟。Liang等[9]提出线路切换的新拓扑攻击方式,采用元启发式优化算法求解攻击模型,但其提出的拓扑攻击方式会对系统造成严重的损失。相比于拓扑攻击,负荷重分配攻击具有更强的隐蔽性,在一定阈值内实施攻击不易引起调度中心的警觉。因此本文主要针对负荷重分配攻击进行研究。Liu等[10]提出虚假数据注入攻击的概念,其构造的攻击可以绕过当时的不良数据检测技术。Yuan等[11]首次提出一种改进虚假数据注入攻击,即LR攻击。LR攻击是一种特殊类型的虚假数据注入攻击,它以系统支路虚假过载为基础干扰安全经济调度。舒隽[12]、Xiang[13−14]等以最大化系统运行成本为目标进行研究,其研究表明虚假数据注入双层优化攻击可能严重危害电力系统安全和经济运行。然而,上述研究未考虑攻击资源的限制及攻击引起的潮流转移会使线路过载,继而导致严重的连锁故障,给电力系统运行造成更大的损失。Che等[15−16]研究了LR攻击对电网造成级联故障的风险并识别了高风险线路,但未能将攻击给电力系统造成的总损失统一度量。以上关于LR攻击的研究均侧重于在电力系统分析攻击效果,且鲜有针对IEGS的信息攻击。Zhao等[4]首次在IEGS中对虚假数据注入攻击进行建模,但其主要研究单一能源子系统被攻击,并未涉及IEGS被协同攻击的情况。Zhao等[17]定义了天然气网中的虚假数据注入攻击,提出了一种日前IEGS协同运行方案来抵御信息攻击的影响,但其主要关注天然气网侧发生的信息攻击,并未考虑可能发生在电网侧的信息攻击。曹茂森等[18]提出了计及连锁故障的电–气耦合系统信息物理协同攻击策略,但其仅在电网侧进行了LR攻击,且未考虑LR攻击资源的限制,也未对系统的脆弱性节点进行分析,不能清晰地反映LR攻击对于IEGS的影响。

综上,本文详细分析在电力–天然气信息物理深度耦合下,双侧协同负荷重分配攻击的机理及流程;计及连锁故障对电力系统造成的影响,建立了LR攻击下的电–气耦合系统损失评估模型,统一度量不同能源子系统中的经济损失,并直观反映双侧协同LR的攻击效果;定义一种新的节点综合脆弱性评估指标,并在不同攻击场景下分析节点的脆弱性变化,进而提出针对不同攻击下的IEGS综合保护策略。仿真验证了保护策略可以有效提高系统抵御攻击的能力,减少系统经济损失。

1 IEGS下LR攻击机理分析

LR攻击是基于传统意义上虚假数据注入攻击的改进,有效避免注入攻击的固有缺点[19],更贴合于实际的信息攻击,对停电风险影响较大[20−21]。因此,本

文提出一种双侧协同LR攻击，对不同能量子系统实施信息攻击。电力–天然气信息物理深度耦合系统由电网、气网、信息网及其通信耦合网络组成。根据复杂网络理论，电网模型采用$E=\{E_G,E_n,E_l\}$，其中，E_G为发电机点集，E_n为负荷点集，E_l为电力线路集。天然气网采用模型$\psi=\{\psi_w,\psi_e,\psi_k,\psi_m,\psi_g\}$表示，其中，$\psi_w$为气源集合，$\psi_e$为气负荷集合，$\psi_k$为压缩机集合，$\psi_m$为天然气管道集合，$\psi_g$为气转电负荷集合。信息网包括了调度中心和各通信节点，负责全网的状态感知及数据采集，信息网采用模型$I=\{I_g,I_e\}$表示，其中，I_g为气网负荷节点的信息子站，I_e为电网负荷节点的信息子站。电–气耦合系统下的双侧协同LR攻击作用机理如图1所示。

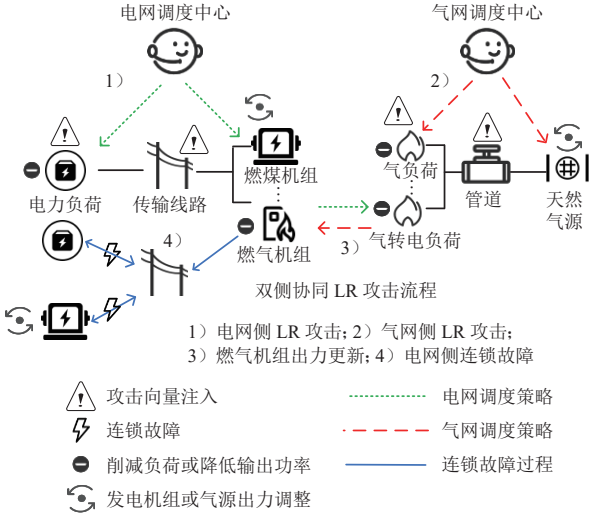


图 1　双侧LR协同攻击机制

Fig. 1　Mechanism of bilateral coordinated LR attack

天然气网与电网通过燃气机组紧密耦合，攻击可以在电–气耦合系统中协同篡改电网和气网的负荷量测数据，诱导不同的调度中心做出错误的调整策略，引起支路或管道过载，从而转移发电机组和气源出力，并且导致系统甩负荷，造成严重的经济损失，危害IEGS安全经济运行。

由图1可知，双侧LR协同攻击过程如下：

1）电网侧 LR 攻击。攻击者在有限攻击资源的约束下先篡改电网侧负荷数据，诱导电网调度中心调整发电机出力和削减负荷，并将调整后的燃气机组出力传导到气网侧参与调度。

2）气网侧 LR 攻击。燃气机组输出功率调整完毕后，攻击者再篡改气网侧负荷量测值，诱导气网侧调度中心做出错误决策，削减气转电负荷和气负荷，使天然气系统处于非经济运行状态。

3）燃气机组出力更新。由于气网侧的攻击会导致气转电负荷严重削减。确定削减后气转电负荷大小，并根据气电转化效率更新燃气机组输出功率。

4）电网侧连锁故障。气转电负荷严重不足会使燃气机组无法参与电网功率自平衡，而燃气机组出力的降低导致电网侧潮流重新平衡[22]，部分过载线路被切除，通过调整燃煤机组出力和切除电力负荷实现功率自平衡。

为突出双侧协同LR攻击效果，本文基于文献[9–21]中的前提假设对部分条件进行简化处理，该处理充分考虑了信息攻击的实际情况及其对IEGS所产生的实质影响[23]。本文在攻击的损失评估中做如下假设：

1）为了使信息攻击的效果更加明显，凸显IEGS的运行风险和脆弱节点，以大多数文献的共通场景为基础进行建模和测试[5–7,11–17]。假设攻击者知晓IEGS的结构参数（如节点导纳矩阵、节点支路矩阵等）和运行方式，并能成功注入虚假数据，躲过状态估计的检测。

2）天然气管存可能会对燃气机组输出功率下降起到缓解作用，但考虑到天然气调度时间尺度远远大于电网调度时间，且管存余量相较于气转电负荷缺口相差甚大，因此可认为管存对保持燃气机组输出功率效果甚微。

3）假设攻击者掌握足够的攻击资源，协同篡改线路和管道潮流量测值作为辅助配合攻击消耗部分资源后，攻击者仍有足量攻击资源用于篡改节点负荷量测值。

2　LR攻击的损失评估模型

负荷损失是LR攻击和连锁故障的直观体现，而由于负荷损失带来的运行成本升高能更真实地反映攻击的危险程度。因此，本文采用攻击后IEGS的总经济损失，统一度量气网侧与电网侧的负荷损失，表征系统抵御攻击的能力。系统经济损失越小，则系统抵御攻击的能力越强。基于攻击者视角建立的LR攻击损失评估模型如图2所示。

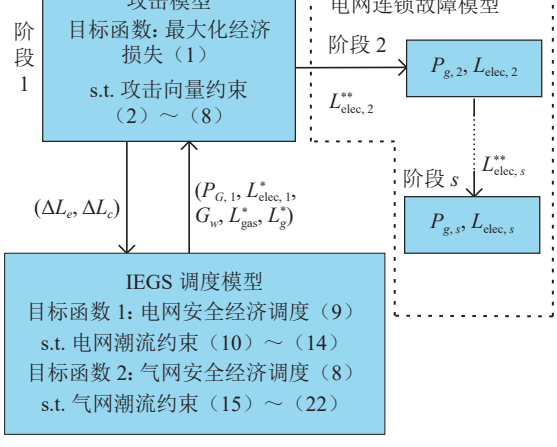


图 2　经济损失评估模型

Fig. 2　Economic loss assessment model

该模型中，攻击者获取IEGS经济运行的参数后，在知晓IEGS系统调度策略的前提下，采用最大化IEGS经济损失的攻击向量进行攻击，其中攻击模型表示攻击者向负荷节点注入虚假数据的行为，IEGS调度模型表示对IEGS中各能源子系统分别进行安全经济调度。攻击者将电网攻击变量ΔL_c注入到电网中，调度模型对电网进行安全经济调度，在秒级的时间尺度下确定阶段1发电机出力$P_{G,1}$和电网切负荷量$L^*_{\text{elec},1}$。之后，将燃气机组输出功率传导至气网侧，配合气网攻击变量ΔL_e参与气网的安全经济调度，在分钟级的时间尺度下确定气源出力G_w、气负荷削减量L^*_{gas}和气转电负荷削减量L^*_g。将变量$P_{G,1}$、$L^*_{\text{elec},1}$、G_w、L^*_{gas}、L^*_g返回攻击模型。阶段2时，根据电网功率自平衡计算支路潮流。如果存在支路潮流过载，则切除过载线路，系统功率重新自平衡后确定燃煤机组出力$P_{g,2}$、电网剩余负荷量$L_{\text{elec},2}$和失电负荷量$L^{**}_{\text{elec},2}$，并进入下一阶段。直到阶段s时，电网功率自平衡后未有过载线路，此时确定燃煤发电机出力$P_{g,s}$、电网剩余负荷量$L_{\text{elec},s}$和失电负荷量$L^{**}_{\text{elec},s}$。

2.1 攻击模型

攻击者在保证LR攻击可以躲过IEGS不良数据检测，知晓IEGS系统调度策略的前提下，以IEGS经济损失最大为目标实施攻击。

2.1.1 攻击模型的目标函数

式(1)计及电网连锁故障对系统负荷的影响，采用经济损失统一度量电网与天然气网的负荷损失，表示攻击模型的目标函数。

$$\max\left(\sum_{i=1}^{N_G}c_1P_{G,1,i}+\sum_{j=1}^{N_{\text{LD}}}c_2L^*_{\text{elec},1,j}+\sum_{k=1}^{N_{\text{GD}}}c_3L^*_{\text{gas},k}+\sum_{s}^{N_s}\sum_{j=1}^{N_{\text{LD}}}c_2L^{**}_{\text{elec},s,j}\right) \tag{1}$$

式中，c_1、c_2、c_3分别为单位发电机组发电成本、电网单位切负荷成本、天然气单位切负荷成本，N_G、N_{LD}、N_{GD}分别为电网中发电机组节点数、电网中负荷节点数、天然气网中负荷节点数，s为电网侧连锁故障的阶段数，N_s为连锁故障传播次数。

2.1.2 攻击约束

LR攻击可在躲过IEGS不良数据检测的同时不引起调度中心的警觉，为此本文建立LR攻击约束的数学模型，如式(2)～(8)所示。式(2)、(3)分别表示电网、气网负荷节点负荷量测值的篡改量代数和为0，保证各系统有功功率和天然气质量平衡。式(4)表示双侧协同攻击下的LR攻击变量。篡改量测值相对于原量测值的比值大小与攻击资源消耗正相关，且近似满足一次相关性[7]，在限定信息攻击资源一定时，LR攻击变量满足约束如式(5)所示。式(6)限制了攻击对单个节点负荷量测值的篡改幅度，以确保攻击可以躲过状态估计的检测。式(7)、(8)分别表示攻击对电网支路、气网管道量测值的篡改量。

$$\sum\Delta L_c=0, c\in I_e \tag{2}$$

$$\sum\Delta L_e=0,\ e\in I_g \tag{3}$$

$$\sum\Delta L_d=\sum\Delta L_c+\sum\Delta L_e, d\in I_g\cup I_e \tag{4}$$

$$\sum\left|\tau\times\frac{\Delta L_d}{L_d}\right|\le R_c,\ d\in I_g\cup I_e \tag{5}$$

$$-\lambda L_d\le\Delta L_d\le\lambda L_d\ , d\in I_g\cup I_e \tag{6}$$

$$\Delta F=-\boldsymbol{S}_1\cdot\boldsymbol{A}_{bl}\cdot\Delta L_c,\ c\in I_e \tag{7}$$

$$\Delta f_{mn}=-\boldsymbol{S}_2\cdot\boldsymbol{G}_{bl}\cdot\Delta L_e,\ e\in I_g \tag{8}$$

式(4)～(8)中，ΔL_d为整个IEGS各节点负荷量测值的篡改量，τ、λ、R_c分别为各负荷节点的攻击难度、单个负荷节点篡改量的阈值上限、LR攻击篡改负荷量测值资源上限，ΔF、Δf_{mn}分别为电网线路和气网管道需要篡改的量测值，$\boldsymbol{S}_1$、$\boldsymbol{S}_2$分别为电网、气网转移因子矩阵，$\boldsymbol{A}_{bl}$、$\boldsymbol{G}_{bl}$分别为电网支路负荷关联矩阵和气网管道负荷关联矩阵。若节点b为支路l的起点，则$\boldsymbol{A}_{bl}=\boldsymbol{G}_{bl}=1$；若母线$b$为支路$l$的终点，则$\boldsymbol{A}_{bl}=\boldsymbol{G}_{bl}=-1$；否则，$\boldsymbol{A}_{bl}=\boldsymbol{G}_{bl}=0$。

2.2 IEGS调度模型

调度人员在满足IEGS中功率平衡、运行约束及系统安全约束的条件下，对IEGS中电网和气网分别进行安全经济调度。

2.2.1 IEGS调度模型的目标函数

IEGS调度模型目标函数如式(9)所示，以最小化电网和气网运行成本为目标分别进行调度。

$$\begin{cases}\left(P_{G,1},L^*_{\text{elec},1}\right)=\arg\left(\min\sum_{i=1}^{N_G}c_1P_{G,1,i}+\sum_{j=1}^{N_{\text{LD}}}c_2L^*_{\text{elec},1,j}\right),\\ \left(L^*_{\text{gas}}\right)=\arg\left(\min\sum_{k=1}^{N_{\text{GD}}}c_3L^*_{\text{gas},k}\right)\end{cases} \tag{9}$$

2.2.2 电网约束条件

1)线路潮流约束为：

$$-F_l^{\max}\le\overline{F}_{l,1}\le F_l^{\max}, l\in E_l \tag{10}$$

式中：$F_l^{\max}$为支路l潮流上限；X_l为线路l的电抗；$\overline{F}_{l,1}$、$\overline{\theta}_{b,1}$分别为电网遭受LR攻击后，运行人员基于所测量的虚假负荷数据进行分析所确定的线路有功潮流和节点相角。$\overline{F}_{l,1}$的表达式为：

$$\overline{F}_{l,1}=\frac{1}{X_l}\sum_{b\in E_n}\boldsymbol{A}_{bl}\bar{\theta}_{b,1},\ l\in E_l \tag{11}$$

2）发电机容量约束为：

$$P_G^{\min}\le P_{G,1}\le P_G^{\max},G\in E_G \tag{12}$$

式中，$P_G^{\max}$、$P_G^{\min}$为发电机出力上下限。

3）电负荷削减量约束为：

$$0\le L_{\text{elec},1}^{*}\le L_{\text{elec},0}+\Delta L_c,\ c\in E_n \tag{13}$$

式中，$L_{\text{elec},0}$为电网初始负荷量。

4）节点功率平衡约束为：

$$\sum_{G\in E_G}P_{G,1}-\sum_{l\in E_l}\boldsymbol{A}_{bl}\overline{F}_l=L_{\text{elec},0}+\Delta L_c-L_{\text{elec},1}^{*},\ c\in E_n \tag{14}$$

2.2.3　天然气网约束条件

1）管道流量约束为：

$$\bar{f}_{mn}|\bar{f}_{mn}|=k_{mn}^2\left(p_m^2-p_n^2\right),\ mn\in\psi_m \tag{15}$$

式中，$\bar{f}_{mn}$为调度人员视角下的管道mn流量，k_{mn}为管道mn流量系数，p_m、p_n分别为节点m、n的气压。

2）节点质量平衡为：

$$\sum_{w\in\psi_w}G_w=\sum_{e\in\psi_e}\left(L_e+\Delta L_e-L_{\text{gas},e}^{*}\right)+\sum_{k\in\psi_m}\theta_k\overline{G}_k+\sum_{mn\in\psi_m}\boldsymbol{G}_{bl}\bar{f}_{mn}+\sum_{g\in\psi_g}\left(L_g-L_g^{*}\right) \tag{16}$$

式中，G_w、L_e、L_g、L_g^{*}分别为气源供应量、气负荷量、气转电负荷量、气转电负荷削减量，$\overline{G}_k$为调度人员视角下的压缩机传输流量，θ_k为压缩机功耗系数，$L_{\text{gas},e}^{*}$为节点气负荷削减量。

3）气负荷消减量约束为：

$$0\le L_{\text{gas},e}^{*}\le L_e+\Delta L_e,\quad e\in\psi_e \tag{17}$$

4）压缩机流量约束为：

$$G_k^{\min}\le\bar{G}_k\le G_k^{\max},\quad k\in\psi_k \tag{18}$$

式中，$G_k^{\max}$、$G_k^{\min}$为压缩机流量上下限。

5）气源出力约束为：

$$G_w^{\min}\le G_w\le G_w^{\max},\quad w\in\psi_w \tag{19}$$

式中，$G_w^{\max}$、$G_w^{\min}$为气源出力上下限。

6）节点气压约束为：

$$p_m^{\min}\le p_m\le p_m^{\max},\quad m\in\psi_e \tag{20}$$

式中，$p_m^{\max}$、$p_m^{\min}$节点m气压上下限。

7）气转电负荷削减约束为：

$$0\le L_g^{*}\le L_g,\quad g\in\psi_g \tag{21}$$

8）燃气机组输出功率约束为：

$$P_{G,\text{gas}}=\eta\left(L_g-L_g^{*}\right),\quad \text{gas}\in E_G,g\in\psi_g \tag{22}$$

式中：η为燃气机组转化效率；$P_{G,\text{gas}}$为燃气机组输出功率，包含在发电机出力$P_{G,1}$内。天然气网通过消耗气转电负荷转化为燃气机组输出功率与电网进行能量交互。

2.3　电网连锁故障模型

攻击会使燃气机组输出功率下降或电网线路过载，导致电网中燃煤发电机组的出力有较大的调整，极易引起连锁故障，危害电网安全[18]。

电网中的连锁故障会使电网拓扑分解为孤岛状态运行，通过电网内的自动发电控制和低频减载装置可以自动平衡孤岛内的机组出力和负荷需求。由于天然气系统运行时间尺度远大于电网，当气网侧的攻击导致气转电负荷不足时，无法在较短时间内调整燃气机组出力，因此只有燃煤机组参与孤岛功率平衡[22]。孤岛平衡策略主要依据系统备用容量v决定。

$$v=\sum_{i=1,j=1}^{N_{\text{BM}}}\left(P_{g,i}^{\max}+P_{G,\text{gas},i}-L_{\text{elec},s,j}\right) \tag{23}$$

式中，$P_{g,i}^{\max}$、$P_{G,\text{gas},i}$、$L_{\text{elec},s,j}$分别为孤岛内各燃煤机组的最大输出功率、阶段s时孤岛内各燃气机组的输出功率、阶段s时孤岛内各节点负荷量，N_{BM}为孤岛的节点数。

1）当$v\ge0$时，孤岛内系统备用容量充足。不同节点处燃煤机组依据剩余发电容量按比例增减出力，如式（24）所示：

$$P_{g,s+1,i}=P_{g,s,i}+\frac{\sum_{i=1,j=1}^{N_{\text{BM}}}\left(L_{\text{elec},s,j}-P_{g,s,i}-P_{G,\text{gas},i}\right)}{\sum_{i=1}^{N_{\text{BM}}}\left(P_{g,i}^{\max}-P_{g,s,i}\right)}\cdot\left(P_{g,i}^{\max}-P_{g,s,i}\right) \tag{24}$$

式中，$P_{g,s,i}$为阶段s时孤岛内各燃煤机组的输出功率。孤岛内各节点负荷量保持不变，如式（25）所示：

$$L_{\text{elec},s+1,j}=L_{\text{elec},s,j},\quad s=2,3,\cdots,N_s \tag{25}$$

2）当$v\le0$，孤岛内备用容量不足。式（26）表示将孤岛内所有燃煤机组出力增至最大，式（27）表示将负荷等比例消减满足功率缺额。

$$P_{g,s+1,i}=P_{g,i}^{\max} \tag{26}$$

$$L_{\text{elec},s+1,j}=L_{\text{elec},s,j}\cdot\left(1-\frac{\sum_{i=1,j=1}^{N_{\text{BM}}}\left(L_{\text{elec},s,j}-P_{g,i}^{\max}-P_{G,\text{gas},i}\right)}{\sum_{j=1}^{N_{\text{BM}}}\left(L_{\text{elec},s,j}\right)}\right),\quad s=2,3,\cdots,N_s \tag{27}$$

调整孤岛内燃煤发电机出力和负荷，得到各节点的净注入功率，运用直流潮流模型计算各支路潮流后，系统功率自平衡。潮流的转移可能会使部分线路越限，从而导致线路停运。如果线路上的潮流大于

其上限时，就将其切除，功率自平衡过程如式（28）～（31）所示。阶段s时的节点功率平衡约束为：

$$\sum_{G\in E_G} P_{G,s} - \sum_{l\in E_l} \boldsymbol{A}_{bl} F_{l,s} = \sum_{j\in E_n} L_{\mathrm{elec},s,j},\ \ s = 2,3,\cdots,N_s \tag{28}$$

式中，$P_{G,s}$为阶段s时电网发电机出力，$F_{l,s}$为阶段s时支路l上的潮流。判断线路l是否被过载切除：

$$|F_{l,s}| \geq F_l^{\max},\ z_l = 0, l \in E_l,\ s = 2,3,\cdots,N_s \tag{29}$$

式中，z_l为支路l的运行状态，$z_l = 1$表示线路l正常运行，$z_l = 0$表示线路l断开。计算连锁故障时的支路潮流为：

$$F_{l,s} = z_l \cdot \frac{1}{X_l} \sum_{b\in E_n} \boldsymbol{A}_{bl}\theta_{b,s},\ \ l \in E_l,\ s = 2,3,\cdots,N_s \tag{30}$$

式中，$\theta_{b,s}$为阶段s时电网节点相角。式（31）表示阶段s时电负荷的切除量。

$$L^{**}_{\mathrm{elec},s,j} = L_{\mathrm{elec},s-1,j} - L_{\mathrm{elec},s,j},\ s = 2,3,\cdots,N_s \tag{31}$$

3 求解方法

3.1 线性化

3.1.1 连锁故障中支路潮流的线性化

连锁故障中的支路潮流是一个非线性函数，通过引入连续变量φ_1～φ_4和0–1变量b_1进行线性化，将约束式（30）线性化得到式（32）：

$$\begin{cases} F_{l,s} = \boldsymbol{A}_{bl}\dfrac{\varphi_1 - \varphi_2}{X_l}, \quad l \in E_l; \\ \varphi_1 = \theta_1 - \varphi_3; \\ \varphi_2 = \theta_2 - \varphi_4; \\ \theta_{\min} \leq \varphi_1 \leq \theta_{\max}; \\ \theta_{\min} \leq \varphi_2 \leq \theta_{\max}; \\ \theta_{\min}(1-b_1) \leq \varphi_3 \leq \theta_{\max}(1-b_1); \\ \theta_{\min}(1-b_1) \leq \varphi_4 \leq \theta_{\max}(1-b_1) \end{cases} \tag{32}$$

式中，θ_1、θ_2分别为l线首端和末端的相位角，$\theta_{\max}$、$\theta_{\min}$分别为最大和最小相位角。

3.1.2 管道流量线性化

天然气网相关节点间的管道流量和压差公式是非线性的。事实上，天然气管道中的流量与气源出力和气负荷相关，其传输损耗较小。为了实现式（15）的线性化，本文利用文献[24]的方法对非线性项进行线性化处理，基于天然气网节点质量平衡计算管道流量。式（33）表示对天然气管道流量上限进行了约束，可以有效确保天然气网安全运行。

$$-f_{mn,\max} \leq \bar{f}_{mn} \leq f_{mn,\max} \tag{33}$$

式中，$f_{mn,\max}$为管道mn流量上限。采用式（33）替代式（15）和（20）参与模型求解。

根据获取的管道流量值和预设的松弛节点压力（选择恒压气源作为松弛节点），可以逐一获取节点压力，可表示为：

$$\begin{cases} p_n = \sqrt{p_m^2 - \left(\bar{f}_{mn}/k_{mn}\right)^2},\ \bar{f}_{mn} \geq 0; \\ p_m = \sqrt{p_n^2 - \left(\bar{f}_{mn}/k_{mn}\right)^2},\ \bar{f}_{mn} \leq 0 \end{cases} \tag{34}$$

求解损失评估模型时，不直接考虑节点压力约束，而是在输出最优解之前进行检验，本文方法在遵循节点气压约束的前提下，简化了损失评估模型的求解。

3.2 Karush–Kuhn–Tucher（KKT）算法

在天然气网管道潮流线性化后，对IEGS调度模型通过KKT条件进行转化，使电–气耦合系统损失评估模型转化为一个带平衡约束的数学规划问题，并将KKT条件作为一组额外的互补约束添加到攻击模型中。KKT算法中的广义拉格朗日函数如下：

$$L(x,\alpha,\beta) = f(x) + \sum_{i=1}^{k} \alpha_i c_i(x) + \sum_{j=1}^{l} \beta_j h_j(x) \tag{35}$$

式中，$f(x)$为IEGS调度模型的目标函数，$c_i(x)$和$h_j(x)$分别为IEGS调度模型中的不等式和等式约束，α_i和β_j分别为拉格朗日不等式和等式乘子，k和l分别为IEGS调度模型中不等式和等式约束的个数，x为IEGS调度模型中的变量。由函数推导的KKT条件如下：

$$\begin{cases} \nabla_x L(x,\alpha,\beta) = 0; \\ \nabla_\alpha L(x,\alpha,\beta) = 0; \\ \nabla_\beta L(x,\alpha,\beta) = 0; \\ \alpha_i c_i(x) = 0, \quad i = 1,2,\cdots,k; \\ c_i(x) \leq 0, \quad i = 1,2,\cdots,k; \\ \alpha_i \geq 0, \quad i = 1,2,\cdots,k; \\ h_j(x) = 0, \quad j = 1,2,\cdots,l \end{cases} \tag{36}$$

采用KKT算法时所引入的拉格朗日乘子会使式（36）中的约束非线性化，借鉴文献[25]的大M法使其线性化。之后，通过式（33）代替式（15）和（20）、式（36）代替IEGS调度模型的约束条件，对电–气耦合系统损失评估模型进行求解；并在求解后，根据式（34）计算和判断节点压力，以对求解可行性进行检验。若可行，则输出结果；否则，调整式（33）参数重新求解。

4 算例分析

本文利用IEEE 39节点电力系统和改进比利时20节点天然气系统组成的电–气耦合系统验证上述损失评估模型。此外，调度中心与发电机组之间的信息联系十分紧密，发电机组的输出功率数据是无法被攻击者篡改的，但这种紧密的信息联系会随着负荷与发电机组距离的增加而减弱[15]，因此，依据系统负荷距离发电机或气源的远近来确定负荷节点的攻击

难度，由参数τ表示[7]，为了更好对比电–气耦合系统所有负荷节点变化情况，现将电、气负荷节点进行统一编号，电网侧负荷节点的编号依次为1～18，气网侧气负荷节点的编号依次为19～25，具体参数见表1。

表 1　负荷节点攻击难度

Tab. 1　Difficulty of load node attack

原有节点	统一编号后的节点	节点攻击难度τ
1	1	1.2
3	2	1.0
4	3	0.8
7	4	1.0
8	5	1.0
9	6	1.2
15	7	0.8
16	8	0.8
18	9	0.8
20	10	1.2
21	11	1.0
23	12	1.2
24	13	1.0
25	14	1.2
26	15	1.0
27	16	0.8
28	17	1.0
29	18	1.2
1	19	1.2
3	20	1.0
6	21	1.0
12	22	1.0
15	23	1.0
19	24	0.8
20	25	0.8

各母线的负荷损失代价为100 \$/MWh，各管道的气负荷损失代价为150 \$/Mm^3。本文在合理化假设的前提下为了凸显攻击效果，将单个负荷节点篡改量的阈值λ设置为0.5[6,7,15]。攻击者若成功发动攻击，则攻击者应掌握足够的攻击资源，篡改线路潮流和管道流量所需的攻击资源不会影响篡改各负荷节点攻击资源的分配，且本文重点研究负荷重分配攻击对IEGS的影响，因此，在算例测试中，暂时不计入篡改线路潮流值所需的攻击资源。本文利用MATLAB实现上述过程，并调用CPLEX求解器进行求解。计算机硬件平台为Inter Core i5–8300H处理器，主频2.3 GHz，内存8 GB。

4.1　不同LR攻击方式对系统运行影响分析

研究3种不同攻击方式对电–气耦合系统运行情况的影响。攻击1，仅从电网侧进行LR攻击；攻击2，仅从气网侧进行LR攻击；攻击3，综合考虑电网侧与气网侧的协同LR攻击。

定义R_c为LR攻击资源上限，选取信息攻击资源为0.7R_c时，分析不同攻击方式对于系统的破坏效果。攻击1、2、3分别对IEGS造成的经济损失为21.99×10^3、29.87×10^3、33.52×10^3 \$。不同攻击形式下系统各节点损失负荷情况如图3所示。

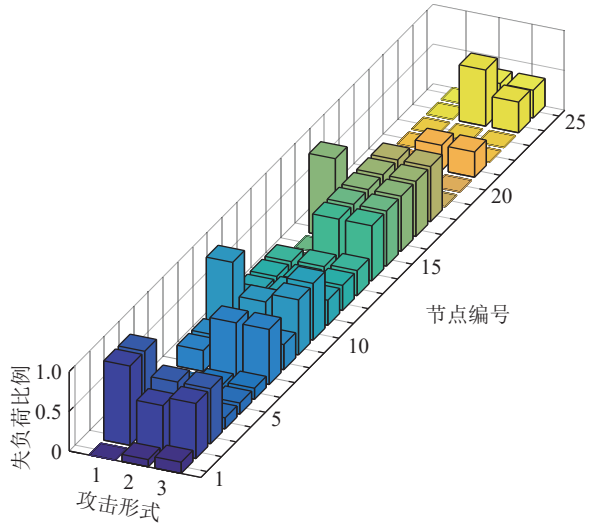


图 3　不同攻击对IEGS的破坏效果

Fig. 3　Destructive effect of different attacks in IEGS

由图3可知，不同攻击方式对于系统运行情况的破坏程度有较大差异。总的来说，采用攻击3对系统的影响最大，攻击2次之，攻击1对系统影响程度最小。说明了在攻击1下，天然气机组具有灵活调节能力，紧急情况下调度中心会优先增加燃气机组的输出，有效解决了电网功率缺额的问题，降低了系统的经济损失；同时，在攻击2、3下，当天然气系统受到攻击或者阻塞时，会优先切断气转电负荷，使燃气机组丧失灵活调节的能力。所以，双侧协同LR攻击会削减增大的气转电负荷，导致燃气机组的输出功率大大降低，不能参与电网功率平衡，因此影响电网侧的安全裕度，从而引发连锁故障，使电网负荷有较大的损失。而相比于攻击2，攻击1并不影响系统的备用容量，则连锁故障后形成的孤岛也更易满足系统功率自平衡的需求，所以攻击1对于系统运行情况的影响最小。

值得注意的是，攻击1中电网侧的部分节点负荷损失比例较高，而在其他两种攻击形式中并未发现节点负荷完全失去的现象。如节点3、4中损失负荷比例达到100%，说明了采用攻击1时，电网侧攻击资源充足，引起更多线路过载，切除过载线路后易形成不含发电机的孤岛，导致节点负荷被全部切除。同时，虽然攻击3会使电网系统的负荷损失大于攻击2的损

失，但在气网侧对于气负荷的削减量却小于攻击2，这是因为攻击资源总量的限制导致攻击3在气网侧分配的资源小于攻击2，所以攻击2会使气网系统的经济损失更大。

4.2 不同攻击资源对系统运行影响分析

为研究不同攻击资源对系统运行情况的影响，比较总攻击资源为$0.5R_c$、$0.6R_c$、$0.7R_c$和$0.8R_c$下系统总经济损失情况。不同攻击资源对于系统的影响情况如图4所示。

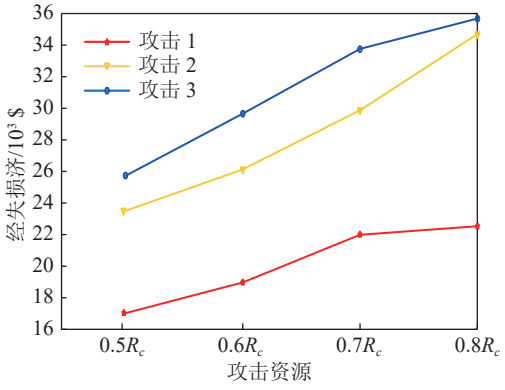


图 4 不同攻击资源下IEGS的经济损失

Fig. 4 Economic loss of IEGS under different attack resources

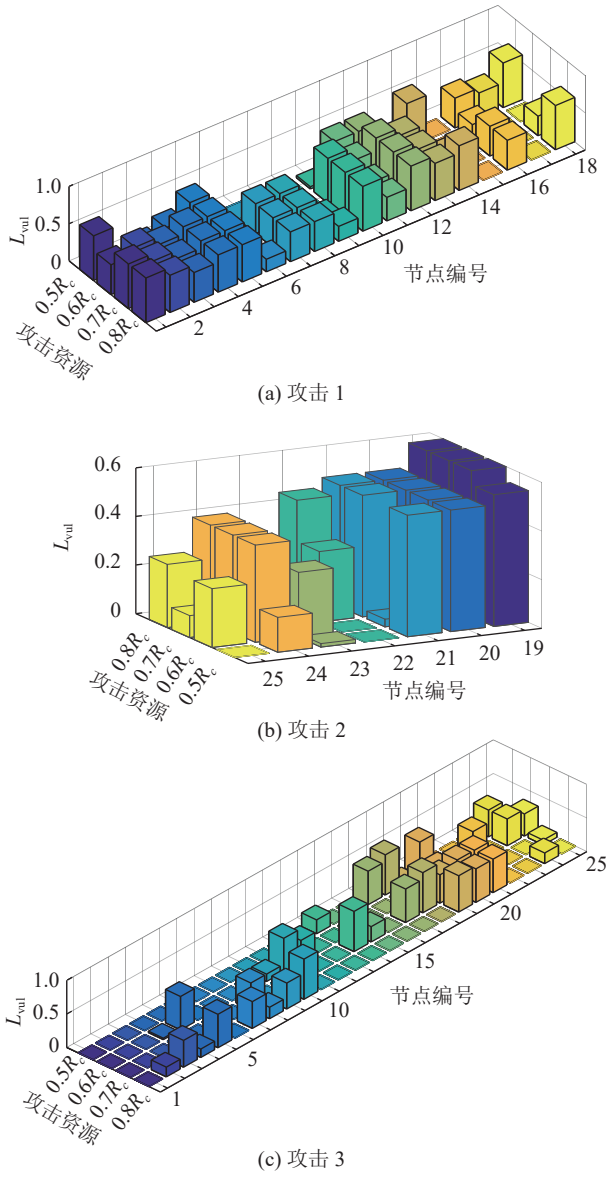
由图4可以看出，同一攻击方式下不同攻击资源时对系统的经济损失具有一定的递进关系，攻击资源越大，对系统造成的经济损失越大。如在攻击资源分别为$0.5R_c$、$0.6R_c$、$0.7R_c$和$0.8R_c$时，攻击2对系统造成损失分别为23.51×10^3、26.13×10^3、29.87×10^3、34.69×10^3 $。显然攻击资源为$0.8R_c$时攻击对系统运行影响最大。对比同一攻击资源下不同的攻击形式可知，当攻击资源较充足时，攻击3对系统造成的损失与攻击2的差值越来越小，如在攻击资源为$0.8R_c$时，攻击2、3对系统造成的经济损失分别为34.69×10^3 $和$35.68\times10^3$ $。表明了攻击2造成气网侧经济损失较多的同时，攻击3中由于总攻击资源的限制，电网侧安全经济调度时燃气机组输出功率增加有限，导致气转电负荷削减量与攻击2接近。因此，攻击2、3在攻击资源较多时对系统造成的经济损失较为相近。

4.3 电–气耦合系统负荷节点脆弱性分析

在信息攻击中，攻击者篡改节点负荷的量测数据，达到破坏电–气耦合系统运行的目的。定义指标L_{vul}表征负荷节点遭受LR攻击的程度，反映节点在LR攻击下的脆弱性，如式(37)所示：

$$L_{\mathrm{vul}}=\left|\tau\times\frac{\Delta L_d}{L_d}\right| \tag{37}$$

图5(a)、(b)和(c)分别给出了不同攻击下各负荷节点的脆弱程度。



(a) 攻击 1

(b) 攻击 2

(c) 攻击 3

图 5 不同攻击下负荷的节点脆弱性

Fig. 5 Vulnerability of load node under different attacks

由图5(a)可知，在攻击1中，随着攻击资源的不断提升，部分负荷节点的脆弱性变化明显。如节点14、18的脆弱性在攻击资源为$0.5R_c$和$0.8R_c$时较高，但在$0.6R_c$和$0.7R_c$时维持在较低水平。表明了在攻击资源总量和一定区域内线路传输容量限制的情况下，不同区域内攻击资源的分配存在一定的波动性。当攻击资源较少时，对于节点18的攻击更容易使系统引发连锁故障，达到切机切负荷、扩大系统经济损失的目的；随着攻击资源的提升，将攻击资源分配给其他区域的负荷节点后对系统造成的损失明显增大，而在攻击资源总量的限制下，分配给节点18的攻击资源会大大减少，因此造成了系统高脆弱性节点的转移；当攻击资源达到$0.8R_c$时，对其他区域内负荷分配的攻击资源趋于饱和，因此又将剩余的资源重新分

配给节点18所在区域的负荷节点，导致节点18重新成为高脆弱性节点。为了使得系统总体经济损失达到最高，攻击资源会优先向满载发电机组的邻接负荷和大负荷节点分配，诱使潮流发生大规模变化和发电机出力转移。如负荷占比较大的节点5和邻接多个发电机组的节点1、12的脆弱性一直保持在较高水平，说明了部分负荷节点会成为攻击的首要目标。

由图5(b)可知，在攻击2中，虽然受到不同攻击资源的影响，系统节点脆弱性并未发生较大改变。如节点19、20、21一直保持较高的脆弱性，表明了攻击若仅发生在气网侧，攻击的主要目标是最大化削减气转电负荷。节点20、21与最大的气转电负荷相邻，给节点20和21分配较多的攻击资源会大幅提高气转电负荷削减量。节点19与负载量最大的气源直接相连，针对节点19的攻击可以使整个气网的气源出力产生有效转移，达到最大化削减气网负荷的效果。

由图5(c)可知，攻击3中系统的高脆弱性节点与攻击1、2相比产生了较大的变化，电网与气网中高脆弱性节点数目的变化体现了攻击资源在电网和气网协同分配的过程。随着攻击资源的增加，在攻击3中系统脆弱性节点转移原理与攻击1、攻击2相同，在此不再赘述。为清晰刻画由于攻击方式的转变而导致系统脆弱性发生的变化，对式(37)的节点脆弱性指标L_{vul}进行修正，如式(38)所示，修正后的A_{vul}指标可以更明确地表征同一负荷节点在不同攻击资源下的脆弱程度，反映了负荷节点的综合脆弱性。

$$A_{\mathrm{vul}}=\sum_{i=1}^{n}\alpha_i\times L_{\mathrm{vul}} \tag{38}$$

式中：A_{vul}为负荷节点的综合脆弱性；n为攻击资源场景个数，本文中n取值为4，α_i为攻击资源i可能出现的概率，满足正态分布规律，其详细参数见表2。

表 2　各攻击场景出现概率

Tab. 2　Probability of each attack scenario

攻击场景	攻击场景出现的概率α_i
$0.5R_c$	0.2
$0.6R_c$	0.3
$0.7R_c$	0.3
$0.8R_c$	0.2

表3给出了采用式(38)计算不同攻击方式下系统各节点的综合脆弱性。

由表3可知，在攻击资源有限的前提下，双侧协同LR攻击中的资源分配给气网侧的比重较高。如节点20的脆弱性达到0.430，高于其他负荷节点，反映了在攻击3中，电网侧的LR攻击主要作用是诱使燃气机组出力提升，真正使系统遭受严重经济损失是依靠LR攻击在气网侧削减气转电负荷，降低燃气机组出力，从而在电网侧引起连锁故障实现的。在攻击1和2中系统高脆弱性节点依次分别为12、1、10、19、20，而攻击3中系统高脆弱性节点排序分别为18、5、17、20、21。可见电网中的高脆弱性节点有较明显的转移，说明不同攻击形式对电网的影响有较大差异。同时，气网中节点的脆弱性有一定的变动，表明了虽然不同攻击在气网中的目标一致，但气转电负荷的变动会改变气网中攻击资源的分配。

表 3　IEGS中节点的综合脆弱性

Tab. 3　Synthesis vulnerability of node in IEGS

节点编号	节点综合脆弱性		
	攻击1	攻击2	攻击3
1	0.540	0	0
2	0.400	0	0.029
3	0.357	0	0.080
4	0.460	0	0.032
5	0.490	0	0.250
6	0.033	0	0
7	0.320	0	0.080
8	0.320	0	0.154
9	0.075	0	0.078
10	0.496	0	0.153
11	0.386	0	0.150
12	0.580	0	0.097
13	0.400	0	0
14	0.322	0	0.222
15	0	0	0.069
16	0.350	0	0
17	0.067	0	0.250
18	0.317	0	0.300
19	0	0.588	0.246
20	0	0.500	0.430
21	0	0.359	0.250
22	0	0.179	0.150
23	0	0.083	0
24	0	0.349	0.232
25	0	0.152	0.135

以上结果表明，当LR攻击资源改变后，系统中的部分高脆弱性节点会发生转移，但仍然有一定比例的负荷节点的脆弱性相对稳定。同时，若改变LR攻击形式，系统的脆弱性节点也会发生较大的转移。所定义的节点综合脆弱性指标有效地反映了不同攻击场景下各节点遭受攻击的程度和高脆弱性节点转移规律。这可以为IEGS防护策略提供相应思路。

4.4　提升系统抵御攻击能力的策略分析

由于LR攻击会对系统安全运行造成严重影响，

为提升系统抵御攻击的能力，提出以下3种针对LR攻击的系统保护策略。策略1，加强保护攻击1、2下系统的高脆弱节点；策略2，加强保护攻击3下系统的高脆弱性节点；策略3，限制气转电负荷的削减比例及加强3种攻击下共同的高脆弱性节点。

采用在负荷节点部署冗余量测装置和增强负荷节点量测冗余度的方式保护脆弱性节点，提升负荷节点被攻击的难度。根据表3中负荷节点在不同攻击形式下的综合脆弱性可知：在策略1中选取节点12、1、19作为保护节点；策略2中节点17、18、20为保护节点；策略3中保护节点为5、18、20，并且将气转电负荷削减比例控制在50%以下。

分别采用3种保护策略后系统经济损失的情况如图6所示。

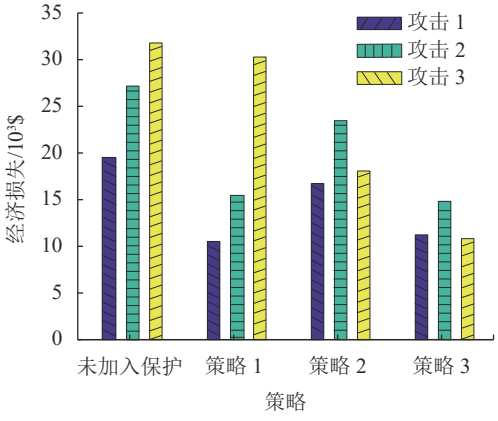


图 6　3种保护策略成效对比

Fig. 6　Effect comparison of three protection strategies

由图6可知，对比加入3种保护策略前后对系统的影响发现，3种保护策略都起到减小系统经济损失，提高系统抵御攻击能力的作用。但对攻击1、2中的高脆弱节点提供保护后，由双侧协同LR攻击造成的系统经济损失并未明显下降，表明保护策略1效果有限，侧面验证了第4.3节中高脆弱性节点转移的正确性。对比3种保护策略，策略3的保护效果显著高于策略1、2，因此，考虑设置气转电负荷削减上限及对共同高脆弱性节点进行保护，可有效减少因LR攻击造成系统严重的经济损失，保障系统安全稳定运行。

5　结　论

本文以电力–天然气信息物理深度耦合系统为研究对象，定量分析了不同LR攻击形式对IEGS造成的经济损失。基于电–气耦合系统的运行特性和双侧协同信息攻击的特点，以负荷重分配的攻击方式最大化系统经济损失，建立损失评估模型，定义新的节点综合脆弱性指标，并提出应对不同攻击的保护策略。仿真结果表明：

1）随着攻击资源的提升，LR攻击对系统造成的损失会进一步加大。但攻击资源提升到一定比例后，攻击对系统造成的经济损失增长缓慢。

2）在攻击资源有限的情况下，合理分配资源对电力系统和天然气系统进行攻击，会使电–气耦合系统遭受最严重的损失；而对脆弱性节点提供保护后，系统抵御攻击能力有所提高。

3）不同的攻击资源和攻击形式都会导致系统的高脆弱性节点发生变化，若只对电网侧LR攻击下的高脆弱性节点进行保护，则双侧协同信息攻击依然会对IEGS造成严重的经济损失。而采用限制气转电负荷的削减比例及加强保护不同攻击下共同高脆弱性节点的策略可以显著提高系统抵御攻击的能力，可为防御者制定合理的防御策略提供重要的依据。

本文在建模时对实际中复杂信息物理系统进行了简化，未考虑以概率模型来表征线路连锁故障，且未计入篡改线路潮流和节点压力所需的攻击资源。因此，下一步将研究信息攻击在电、热（冷）、气等多能源系统的作用方式，采用分布式算法，在更大规模的综合能源系统中建立精细的模型。

参考文献：

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

[2] Guo Qinglai,Xin Shujun,Wang Jianhui,et al.Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine's blackout[J].Automation of Electric Power Systems,2016,40(5):145–147.[郭庆来,辛蜀骏,王剑辉,等.由乌克兰停电事件看信息能源系统综合安全评估[J].电力系统自动化,2016,40(5):145–147.]

[3] Yang Zijuan,Gao Ciwei,Zhao Ming.Review of coupled system between power and natural gas network[J].Automation of Electric Power Systems,2018,42(16):21–31.[杨自娟,高赐威,赵明.电力–天然气网络耦合系统研究综述[J].电力系统自动化,2018,42(16):21–31.]

[4] Zhao Pengfei,Gu Chenghong,da Huo.Coordinated risk mitigation strategy for integrated energy systems under cyber-attacks[J].IEEE Transactions on Power Systems,2020,35(5):4014–4025.

[5] Tian Meng,Dong Zhengcheng,Wang Xianpei,et al.Analysis of electrical coordinated cyber physical attacks under goal conflict[J].Power System Technology,2019,43(7):2336–2344.[田猛,董政呈,王先培,等.目标冲突下电力信息物理协同攻击分析[J].电网技术,2019,43(7):2336–2344.]

[6] Fu Jian,Hu Bo,Xie Kaigui,et al.Stochastic planning of generation and transmission expansion for power system

against coordinated attacks[J].Automation of Electric Power Systems,2021,45(2):21–29.[伏坚,胡博,谢开贵,等.应对协同攻击的电力系统发输电拓展随机规划[J].电力系统自动化,2021,45(2):21–29.]

[7] 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.[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.]

[8] Wang Chaochao,Dong Xiaoming,Sun Hua,et al.Modeling method of power cyber-physical system considering multi-layer coupling characteristics[J].Automation of Electric Power Systems,2021,45(3):83–91.[王超超,董晓明,孙华,等.考虑多层耦合特性的电力信息物理系统建模方法[J].电力系统自动化,2021,45(3):83–91.]

[9] Liang Gaoqi,Weller S R,Zhao Junhua,et al.A framework for cyber-topology attacks:Line-switching and new attack scenarios[J].IEEE Transactions on Smart Grid,2019,10(2):1704–1712.

[10] Liu Yao,Ning Peng,Reiter M K.False data injection attacks against state estimation in electric power grids[C]//CCS'09:Proceedings of the 16th ACM conference on Computer and communications security.New York:ACM,2009:21–32.

[11] Yuan Yanling,Li Zuyi,Ren Kui.Modeling load redistribution attacks in power systems[J].IEEE Transactions on Smart Grid,2011,2(2):382–390.

[12] Shu Jun,Guo Zhifeng,Han Bing.Bi-level optimization model of false data injection attack for power grid[J].Automation of Electric Power Systems,2019,43(10):95–100.[舒隽,郭志锋,韩冰.电网虚假数据注入攻击的双层优化模型[J].电力系统自动化,2019,43(10):95–100.]

[13] Xiang Yingmeng,Ding Zhilu,Zhang Yichi,et al.Power system reliability evaluation considering load redistribution attacks[J].IEEE Transactions on Smart Grid,2017,8(2):889–901.

[14] Xiang Yingmeng,Wang Lingfeng.A game-theoretic study of load redistribution attack and defense in power systems[J].Electric Power Systems Research,2017,151:12–25.

[15] 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.

[16] Che Liang,Liu Xuan,Shuai Zhikang,et al.Cyber cascades screening considering the impacts of false data injection attacks[J].IEEE Transactions on Power Systems,2018,33(6):6545–6556.

[17] Zhao Bining,Lamadrid A J,Blum R S,et al.A coordinated scheme of electricity-gas systems and impacts of a gas system FDI attacks on electricity system[J].International Journal of Electrical Power & Energy Systems,2021,131:107060.

[18] Cao Maosen,Wang Leibao,Hu Bo,et al.Coordinated cyber-physical multi-stage attack strategy considering cascading failure of integrated electricity–natural gas system[J].Electric Power Automation Equipment,2019,39(8):128–136.[曹茂森,王蕾报,胡博,等.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[J].电力自动化设备,2019,39(8):128–136.]

[19] Lee L,Hu Po.Vulnerability analysis of cascading dynamics in smart grids under load redistribution attacks[J].International Journal of Electrical Power & Energy Systems,2019,111:182–190.

[20] Deng Ruilong,Xiao Gaoxi,Lu Rongxing,et al.False data injection on state estimation in power systems—Attacks,impacts,and defense:A survey[J].IEEE Transactions on Industrial Informatics,2017,13(2):411–423.

[21] 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.

[22] Zhang Anan,Li Jing,Lin Dong,et al.A cascading failure model of electricity–gas coupling system considering the influence of limit risk of natural gas pipeline network[J].Proceedings of the CSEE,2021,41(21):7275–7285.[张安安,李静,林冬,等.考虑天然气管网极限风险影响的电–气耦合系统连锁故障模型[J].中国电机工程学报,2021,41(21):7275–7285.]

[23] Liang Gaoqi,Weller S R,Zhao Junhua,et al.The 2015 Ukraine blackout:Implications for false data injection attacks[J].IEEE Transactions on Power Systems,2017,32(4):3317–3318.

[24] Li Guoqing,Zhang Rufeng,Jiang Tao,et al.Security-constrained bi-level economic dispatch model for integrated natural gas and electricity systems considering wind power and power-to-gas process[J].Applied Energy,2017,194:696–704.

[25] He Chuan,Wu Lei,Liu Tianqi,et al.Robust co-optimization scheduling of electricity and natural gas systems via ADMM[J].IEEE Transactions on Sustainable Energy,2017,8(2):658–670.

（编辑　赵　婧）

引用格式：Zhou Buxiang,Min Xinwei,Zang Tianlei,et al.Loss assessment and vulnerability analysis of an integrated electricity natural gas system under load redistribution attack[J].Advanced Engineering Sciences,2023,55(1):3–13.[周步祥,闵昕玮,臧天磊,等.负荷重分配攻击下电–气系统损失评估与脆弱性分析[J].工程科学与技术,2023,55(1):3–13.]