DOI:10.12158/j.2096-3203.2023.04.010

面向交直流混联电网的虚假数据注入攻击策略优化

谢云云[1]，严欣腾[2]，燕子敖[1]，桑梓[3]，袁晓舒[3]
（1. 南京理工大学自动化学院，江苏 南京 210094；2. 中铁上海设计院集团有限公司，
上海 200072；3. 东方电气集团科学技术研究院有限公司，四川 成都 611731）

摘　要：虚假数据注入（false data injection，FDI）攻击是对电力系统运行影响较为严重的一种攻击。目前已有对交直流混联电网的 FDI 攻击方法的研究，但仍缺乏对交直流混联电网攻击策略的优化研究。为此，文中提出了面向交直流混联电网的 FDI 攻击策略优化方法。首先，建立以 FDI 攻击损失最大为目标的双层优化模型，上层模型以电力系统经济损失最大为目标对 FDI 攻击策略进行优化；下层模型以发电机出力调整量和切负荷量最小为目标计算 FDI 攻击下的最大经济损失，考虑交直流混联电网安全约束和换相失败风险。然后，采用遗传算法对优化模型进行求解，生成最优攻击策略。最后，以改进的 IEEE 14 节点系统为例验证了模型的有效性。仿真结果表明，优化后的攻击策略能够显著提高安全约束经济调度（security constrained economic dispatch，SCED）的运行成本。

关键词：交直流混联电网；虚假数据注入（FDI）攻击；换相失败；遗传算法；优化模型；安全约束经济调度（SCED）
中图分类号：TM743　　**文献标志码**：A　　**文章编号**：2096-3203（2023）04-0094-08

0　引言

电力系统的安全稳定运行是社会经济稳定和国民经济发展的基础[1]。电力系统物理网络和信息网络的高度融合，使得现代电力系统发展成为信息、物理融合的电力系统[2-3]。这提高了电力系统的控制水平，但同时也使电力系统面临网络恶意攻击的风险[4-7]。在各种网络攻击[8-12]中，虚假数据注入（false data injection，FDI）攻击针对数据采集与监视系统中的状态估计单元，通过恶意篡改量测数据干扰状态估计结果，误导系统操作员的决策，使攻击者达到破坏系统或是获取经济利益的目的。FDI 攻击实施成本低、隐蔽性高、攻击范围广，对电力系统安全经济运行造成威胁。随着近年来高压直流输电线路投运数量的不断增加，电网逐渐发展成交直流混联电网[13-14]。对交直流混联电网的 FDI 攻击策略进行研究，能够更好地防御 FDI 攻击，提高交直流混联电网运行的安全性。

现有的大多数关于 FDI 攻击的研究都是基于攻击者了解相关的系统配置信息。攻击者在构造攻击向量时，考虑到攻击成本等限制，对最小的攻击集合进行了优化[15-16]。也有学者研究在无法获取电网完整信息情况下的攻击。文献[17]利用公开的市场数据恢复了网络拓扑，文献[18]提出了一种基于线性独立量分析的网络拓扑推断算法。文献[19]表明攻击者只须获取局部攻击区域的拓扑和参数信息就可以设计出虚假数据，没有必要知道任何关于非攻击区域的网络信息。

为了解攻击者行为特征与量测系统的脆弱点，有学者从攻击效果的角度优化了 FDI 攻击。文献[20]将攻击前后量测值之差的平方和作为目标函数，使攻击后的量测值尽可能偏离实际的量测值。但这种衡量指标没有考虑电网工作人员的行为特征。由于状态估计结果会对考虑安全约束经济调度（security constrained economic dispatch，SCED）的安全控制策略产生影响，文献[21]在文献[20]的基础上，将 SCED 成本作为衡量攻击效果的指标，建立了双层优化模型，并采用 KKT 方法求解。文献[22]将负荷再分配攻击分为即时攻击与延时攻击，同样考虑了经济调度的成本。文献[23]提出了一种基于博弈论的关键测量设备分阶段动态防御方法，采用最优负荷减载算法量化攻击效果。文献[24]以交直流混联电网作为研究场景，构建了 FDI 的攻击模型。文献[25]建立了 FDI 攻击的双层模型，通过加权的电能损失和线路越限来量化攻击效果，并对攻击资源进行约束，使之更加贴近实际。

然而，现有 FDI 攻击策略针对的主要是交流系统，文献[24]提出了面向交直流混联电网的 FDI 攻击方法，但未对 FDI 攻击策略进行优化。因此，文中进一步提出了面向交直流混联电网的 FDI 攻击策略优化方法。以现有的交直流混联电网状态估计交替迭代算法为基础，建立了面向交直流混联电网的 FDI 攻击策略优化模型。模型考虑了直流系统换相失败，假设发生攻击后系统操作人员能根据错误的

收稿日期：2022-12-18；修回日期：2023-02-13
基金项目：国家自然科学基金资助项目（52177090）

状态估计结果进行 SCED,并以 SCED 的成本来量化攻击效果。最后采用遗传算法对优化模型进行求解,并以改进的 IEEE 14 节点系统为例对模型的有效性进行验证。

1 面向交直流混联电网的 FDI 攻击方法

文献[24]对攻击模型的描述较为详细,因篇幅所限,文中对此只做简单描述,以图 1 为例说明攻击模型。V_1、V_2、V_3、V_4分别为节点 1、2、3、4 的电压幅值;θ_1、θ_2、θ_3、θ_4分别为节点 1、2、3、4 的电压相角;红线表示该线路为直流线路,其中节点 1 为整流侧,节点 4 为逆变侧;黑色箭头表示节点负荷。

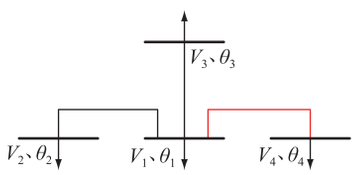

图 1 发生在换流母线的攻击说明

Fig.1 Illustration of an attack on a converter bus

1.1 攻击换流母线电压幅值

假设攻击者想将节点 1 电压幅值 V_1 的估计值改变大小 V_1',而其他状态变量在攻击前后保持不变,需要改变与节点 1 直接相连节点的有功、无功注入功率,即 P_1、Q_1、P_2、Q_2、P_3、Q_3,以及与节点 1 直接相连支路的有功、无功功率潮流,即 $P_{1,2}$、$Q_{1,2}$、$P_{1,3}$、$Q_{1,3}$。

对于交流部分,以节点 1 与节点 2 之间的有功、无功功率潮流 $P_{1,2}$与 $Q_{1,2}$为例,假设 $P_{1,2}$、$Q_{1,2}$ 需要篡改的大小分别为 $P'_{1,2}$、$Q'_{1,2}$,其数值可以由式(1)、式(2)确定。

$$\begin{aligned}P'_{1,2}=P''_{1,2}-P_{1,2}=&(V_1+V_1')^2g_{1,2}-\\&(V_1+V_1')V_2(g_{1,2}\cos\theta_{1,2}+b_{1,2}\sin\theta_{1,2})-\\&V_1^2g_{1,2}+V_1V_2(g_{1,2}\cos\theta_{1,2}+b_{1,2}\sin\theta_{1,2})\end{aligned}\tag{1}$$

$$\begin{aligned}Q'_{1,2}=Q''_{1,2}-Q_{1,2}=&-(V_1+V_1')^2(b_{1,2}+b_{1,2}^{\mathrm{sh}})-\\&(V_1+V_1')V_2(g_{1,2}\sin\theta_{1,2}-b_{1,2}\cos\theta_{1,2})+\\&V_1^2(b_{1,2}+b_{1,2}^{\mathrm{sh}})+V_1V_2(g_{1,2}\sin\theta_{1,2}-b_{1,2}\cos\theta_{1,2})\end{aligned}\tag{2}$$

式中:$P''_{1,2}$、$Q''_{1,2}$分别为受攻击后节点 1 与节点 2 之间支路的有功、无功功率潮流;$g_{1,2}$、$b_{1,2}$ 分别为线路 1—2 的电导和电纳;$b_{1,2}^{\mathrm{sh}}$为对地电纳;$\theta_{1,2}$为节点 1 和节点 2 之间的相角差,即 $\theta_{1,2}=\theta_1-\theta_2$。

同理可以确定节点 1 与节点 3 之间需要篡改的有功、无功功率潮流量测量 $P'_{1,3}$、$Q'_{1,3}$。

节点 1 需要篡改的注入功率大小可由式(3)、式(4)确定。

$$P'_1=P''_1-P_1=P'_{1,2}+P'_{1,3}\tag{3}$$

$$Q'_1=Q''_1-Q_1=Q'_{1,2}+Q'_{1,3}+Q'_{\mathrm{acr}}\tag{4}$$

式中:P'_1、Q'_1 分别为节点 1 需要篡改的有功、无功注入功率大小;P''_1、Q''_1分别为受攻击后节点 1 的有功、无功注入功率;Q'_{acr}为需要篡改的直流部分整流侧无功功率。

同理可以确定节点 2 与节点 3 中,需要篡改的有功、无功注入功率大小 P'_2、Q'_2、P'_3、Q'_3。

对于直流部分,需要篡改的整流侧无功功率 Q'_{acr} 可以由式(5)确定。

$$Q'_{\mathrm{acr}}=\sqrt{3}(V_1+V_1')I_{\mathrm{acr}}\sin(\boldsymbol{\Phi}_{\mathrm{r}}+\boldsymbol{\Phi}'_{\mathrm{r}})-\sqrt{3}V_1I_{\mathrm{acr}}\sin\boldsymbol{\Phi}_{\mathrm{r}}\tag{5}$$

式中:I_{acr} 为交流侧电流;$\boldsymbol{\Phi}_{\mathrm{r}}$、$\boldsymbol{\Phi}'_{\mathrm{r}}$分别为受攻击前、后整流侧功率因数角。

由上述公式能够确定攻击向量 $\boldsymbol{a}$。当攻击者利用 $\boldsymbol{a}$ 展开 FDI 攻击时,能够实现将节点 1 电压幅值的估计值改变 V_1' 的目的,并能绕过不良数据检测。

1.2 攻击换流母线电压相角

假设攻击者想要将节点 1 的电压相角 θ_1 的估计值改变大小 θ_1',而其他状态变量在攻击前后保持不变。由于换流母线电压相角的改变不影响直流部分的量测量,因此攻击者无须篡改直流部分的量测量,即直流部分的攻击向量为 $\boldsymbol{0}$。$P'_{1,2}$、$Q'_{1,2}$的大小可以由式(6)、式(7)确定。

$$\begin{aligned}P'_{1,2}=P''_{1,2}-P_{1,2}=&\\V_1^2g_{1,2}-V_1V_2g_{1,2}\cos(\theta_{1,2}+\theta_1')-&\\V_1V_2b_{1,2}\sin(\theta_{1,2}+\theta_1')-V_1^2g_{1,2}+&\\V_1V_2g_{1,2}\cos\theta_{1,2}+V_1V_2b_{1,2}\cos\theta_{1,2}&\end{aligned}\tag{6}$$

$$\begin{aligned}Q'_{1,2}=Q''_{1,2}-Q_{1,2}=&\\-V_1^2(b_{1,2}+b_{1,2}^{\mathrm{sh}})-V_1V_2g_{1,2}\sin(\theta_{1,2}+\theta_1')+&\\V_1V_2b_{1,2}\cos(\theta_{1,2}+\theta_1')+V_1^2(b_{1,2}+b_{1,2}^{\mathrm{sh}})+&\\V_1V_2g_{1,2}\sin\theta_{1,2}-V_1V_2b_{1,2}\cos\theta_{1,2}&\end{aligned}\tag{7}$$

同理可以确定节点 1 与节点 3 之间需要篡改的有功、无功功率潮流量测量 $P'_{1,3}$、$Q'_{1,3}$。

节点 1 需要篡改的有功、无功注入功率大小由式(3)与式(4)确定。同理可以确定其他节点的功率注入大小。

根据上述公式,可以实现节点 1 电压相角的估计值改变 θ_1' 的目的,并能绕过不良数据检测。

上述 FDI 攻击方法也适用于多个节点状态变量估计值的改变,并且可以同时改变电压幅值和电压相角的估计值。

2 FDI 攻击策略双层优化模型

第 1 章中针对交直流混联电网的 FDI 攻击方法

仅能实现 FDI 攻击，并未考虑开展攻击对系统运行的影响。因此，须对该攻击策略进行优化，建立面向交直流混联电网的 FDI 攻击策略双层优化模型。

2.1 上层模型

2.1.1 上层模型目标函数

在攻击策略不被状态估计方法发现的前提下，攻击需要最大化交直流混联电网的经济损失。文中以电力系统经济调度后总成本最大为目标对 FDI 攻击策略进行优化，其中总成本 f 包括了发电成本和切负荷成本，如式(8)所示。

$$\max f = \sum_{i=1}^{I_1} c_{G,i}\bar{P}_{G,i} + \sum_{j=1}^{I_2} c_{S,j}\bar{P}_{S,j} \tag{8}$$

式中：$\bar{P}_{G,i}$ 为节点 i 上机组经过 SCED 后的发电调整量；$c_{G,i}$ 为节点 i 上机组的发电成本；$\bar{P}_{S,j}$ 为节点 j 经过 SCED 后的切负荷量；$c_{S,j}$ 为节点 j 的切负荷成本；I_1 为机组节点集合；I_2 为负荷节点集合。

2.1.2 上层模型约束条件

(1) 不良数据检测约束。攻击者开展 FDI 攻击，状态估计器以被篡改的量测数据作为输入，通过现有研究中常用的残差 2-范数来检测不良数据[21]。不良数据检测结果处于门槛值之内是攻击者能够成功实施 FDI 攻击的前提。该约束可表示为：

$$\| \boldsymbol{z}' - \boldsymbol{h}(\hat{\boldsymbol{x}}') \|_2 < \tau \tag{9}$$

式中：$\hat{\boldsymbol{x}}'$ 为受攻击后状态变量估计值；$\boldsymbol{h}(\hat{\boldsymbol{x}}')$ 为用状态变量 $\hat{\boldsymbol{x}}'$ 来表示量测量的量测方程；$\boldsymbol{z}'$ 为受攻击后被篡改的量测量；τ 为不良数据检测的门槛值。由于量测方程的具体表达式有 18 个方程，为减小篇幅，文中未详细列出，具体可见文献[24]。

(2) 量测数据攻击范围约束。当篡改的量测数据过大时，将很容易被检测出来，因此，篡改的量测数据大小须在攻击量正常运行的范围内。

$$z_{k,\min} \leqslant z'_k \leqslant z_{k,\max} \tag{10}$$

式中：z'_k 为第 k 个受攻击后被篡改的量测量；$z_{k,\max}$、$z_{k,\min}$ 分别为第 k 个受攻击量的上、下限。

由于篡改的量测量过大，通过状态估计不良数据检测机制或通过与历史数据对比，会比较容易被检测出来。假设有功、无功功率注入量测量被篡改的大小不超过原量测值的±50%，而支路有功、无功功率潮流量测量不超出线路最大容量[21,25]。对于零负荷节点和发电机节点，则无法对其攻击，因为容易被检测出来。

2.2 下层模型

2.2.1 下层模型目标函数

在开展 FDI 攻击时，操作人员会根据状态估计的结果进行 SCED，在满足功率平衡约束、电压安全约束、机组运行约束等条件下调整机组出力和进行切负荷操作，以实现系统安全经济运行。其目标函数为：

$$(\bar{P}_{G,i},\bar{P}_{S,j}) = \underset{P_{G,i},P_{S,j}}{\operatorname{argmin}} \left(\sum_{i=1}^{I_1} c_{G,i}P_{G,i} + \sum_{j=1}^{I_2} c_{S,j}P_{S,j} \right) \tag{11}$$

式中：$P_{G,i}$ 为节点 i 上机组的发电量；$P_{S,j}$ 为节点 j 的切负荷量。

2.2.2 下层模型约束条件

(1) 功率平衡约束。

$$P_{G,i} - (P'_{D,i} - P_{S,j}) - V_i \times \sum_{j\in S_i} V_j(g_{i,j}\cos\theta_{i,j} + b_{i,j}\sin\theta_{i,j}) + mP'_{acr(i)} = 0 \tag{12}$$

$$Q_{G,i} - Q'_{D,i} - V_i \sum_{j\in S_i} V_j(g_{i,j}\sin\theta_{i,j} - b_{i,j}\cos\theta_{i,j}) - tQ'_{acr(i)} = 0 \tag{13}$$

式中：$P'_{D,i}$、$Q'_{D,i}$ 分别为受攻击后状态估计输出的节点 i 上的有功、无功负荷量测量；S_i 为与节点 i 相连节点的集合；$Q_{G,i}$ 为节点 i 上机组的无功输出；V_i、V_j 分别为节点 i、j 的电压幅值；$g_{i,j}$、$b_{i,j}$ 分别为支路 i—j 的电导和电纳；$\theta_{i,j}$ 为节点 i 和节点 j 之间的相角差；$P'_{acr(i)}$、$Q'_{acr(i)}$ 分别为受攻击后状态估计输出的整流侧(逆变侧)的直流有功、无功量测量，其中下标为 r 时表示整流侧，下标为 i 时表示逆变侧。m、t 均为常数，当节点 i 为整流侧时，m 取−1，t 取 1；当节点 i 为逆变侧时，m、t 均取 1；当节点 i 为非换流母线节点时，m、t 均取 0。

(2) 机组出力约束。

$$P_{G,i\min} < P_{G,i} < P_{G,i\max} \tag{14}$$

$$Q_{G,i\min} < Q_{G,i} < Q_{G,i\max} \tag{15}$$

式中：$P_{G,i\max}$、$P_{G,i\min}$ 分别为节点 i 上机组的有功上、下限；$Q_{G,i\max}$、$Q_{G,i\min}$ 分别为节点 i 上机组的无功上、下限。

(3) 切负荷约束。所切负荷量应不大于受攻击后状态估计得到的负荷量测量 $P'_{D,j}$。

$$0 \leqslant P_{S,j} \leqslant P'_{D,j} \tag{16}$$

(4) 支路潮流约束。

$$S_{i,j\min} \leqslant S_{i,j} \leqslant S_{i,j\max} \tag{17}$$

式中：$S_{i,j\max}$、$S_{i,j\min}$ 分别为支路 i—j 视在功率上、下限；$S_{i,j}$ 为支路 i—j 的视在功率。

(5) 节点电压约束。

$$V_{i,\min} < V_i < V_{i,\max} \tag{18}$$

式中：$V_{i,\max}$、$V_{i,\min}$ 分别为节点 i 电压幅值上、下限。

(6) 节点相角约束。

$$\theta_{i,\min} < \theta_i < \theta_{i,\max} \tag{19}$$

式中:$\theta_{i,\max}$、$\theta_{i,\min}$分别为节点i电压相角上、下限。

2.2.3 考虑换相失败风险

当系统操作员根据计算结果实施调度后,由于实际的负荷量与受攻击后状态估计输出的负荷量存在偏差,根据错误的状态估计结果实施调度,可能会导致换流母线电压降低,引起直流换流站换相失败。引起直流换流站换相失败的临界换相电压可以表示为:

$$U_{\mathrm{Lmin}}=U_{\mathrm{L0}}\sqrt{\frac{\cos^2\gamma_0-\cos^2\beta_0}{\cos^2\gamma_{\min}-\cos^2\beta_0}} \tag{20}$$

式中:U_{Lmin}为临界换相电压;U_{L0}为换相电压初始有效值;γ_0为逆变侧初始熄弧角;$\gamma_{\min}$为逆变侧极限熄弧角;β_0为逆变侧初始超前角。

当系统操作员根据优化模型得到的最优攻击策略进行调度时,若逆变侧换流母线节点电压幅值低于临界换相电压,则可认为直流站换相失败。此时,若重新进行SCED,则会使调度成本进一步增加。

2.3 模型求解

文中采用遗传算法来解决FDI攻击策略优化问题,将状态估计与SCED算法分别采用遗传算法进行寻优,求取最优攻击策略,求解的流程见图2。

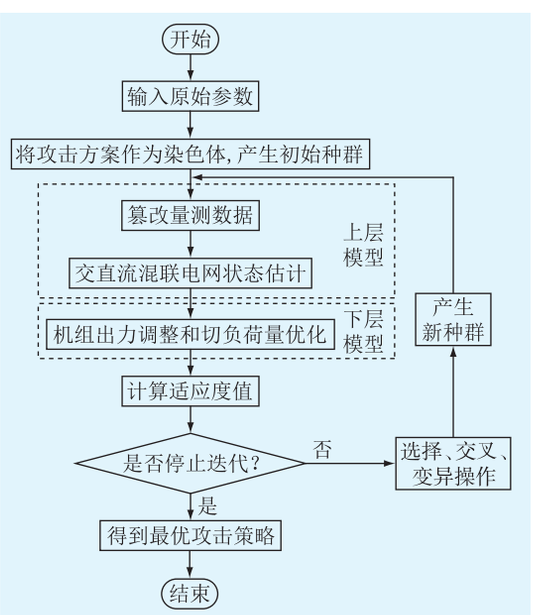

图2 优化模型求解流程

Fig.2 Flow chart of optimization model solution

结合图2和遗传算法基本原理,介绍上层模型求解步骤。下层模型的求解过程与上层模型类似,文中不再赘言。遗传算法的执行过程如下:

(1)产生初始种群。初始种群中的每个个体代表一个攻击方案,即系统中所有量测量的集合。量测量在取值范围内随机生成,组合成不同的攻击方案。

(2)适应度函数。适应度函数根据所求问题的目标函数来确定,文中以SCED的成本作为适应度函数,不同的攻击策略对应不同的适应度。对于攻击者来说,适应度越大的攻击策略所产生的攻击效果越好。在计算SCED成本时,需要使用下层模型的求解结果。采用上层模型中的攻击方案,以及与上层模型相同的遗传算法,可以求得下层模型优化结果。下层模型结果返回给上层优化模型,以计算其适应度值。

(3)根据适应度大小对个体进行选择和繁殖。自然界中,越适应的个体就越有可能存活下来,并繁殖后代,即适应度越大的个体能产生的后代越多。个体选择通常采用轮盘赌法。

(4)交叉运算。对于选择运算繁衍得到的个体,以一定的概率进行两两之间的算数交叉运算。

(5)变异运算。对于要进行变异运算的每个个体,将需要变异的基因以一定的概率重新随机选取新值。

(6)停止迭代条件。在迭代K次后,选择所得种群中适应度最大的个体作为最终解,即最后的最优攻击策略。

3 算例分析

3.1 算例场景

文中以改进的IEEE 14节点系统对基于交替迭代法的交直流混联电网状态估计进行仿真分析,仿真系统如图3所示。图3中,将原有的交流线路4—5替换为高压直流输电线路,如图中红色部分所示,其中节点5连接整流侧,节点4连接逆变侧。

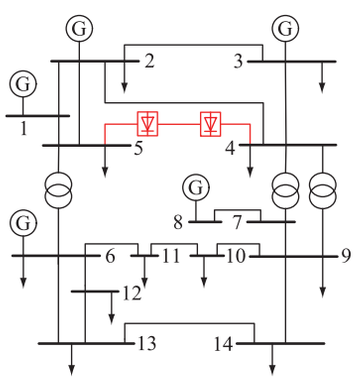

图3 改进的IEEE 14节点系统

Fig.3 Improved IEEE 14-bus system

两端直流输电系统参数如下:换流变压器变比为525 kV/209 kV,电抗为220 Ω;换流器直流电压额定值为500 kV,直流电压最大值为525 kV;整流器超前触发角α范围为5°~57°,额定触发角为15°;

逆变侧熄弧角 γ 为 16°，极限熄弧角为 15°；直流输电线路电阻为 50 Ω，直流输送容量为 30 000 MW。

由于 IEEE 14 节点系统交流部分状态估计采用标幺值，而直流部分状态估计采用有名值，为使程序计算方便，须将交流部分换流母线电压转化为有名值，作为直流部分的输入；将直流部分的有功、无功功率转化为标幺值，作为交流部分的输入。其中，节点 1~5 的电压等级为 500 kV，电压有名值为标幺值乘以 525；节点 6~14 的电压等级为 220 kV，电压有名值为标幺值乘以 230；基准功率为 100 MW，功率有名值为标幺值乘以 100。线路参数和变压器参数如表 1 和表 2 所示。表 1 中的对地导纳为二分之一的对地电纳。状态估计量测配置如表 3 所示，其中量测类型 1 为节点电压幅值量测量；量测类型 2、3 分别为节点有功、无功功率注入量测量；量测类型 4、5 分别为支路有功、无功潮流量测量。

表 1 线路参数

Table 1 Line parameters p.u.

首端节点	末端节点	支路电阻	支路电抗	对地导纳
1	2	0.019 38	0.059 17	0.026 4
1	5	0.054 03	0.223 04	0.024 6
2	3	0.046 99	0.197 97	0.021 9
2	4	0.058 11	0.176 32	0.018 7
2	5	0.056 95	0.173 88	0.017 0
3	4	0.067 01	0.171 03	0.017 3
4	5	0.013 35	0.042 11	0.006 4
6	11	0.094 98	0.198 90	0
6	12	0.122 91	0.255 81	0
6	13	0.066 15	0.130 27	0
7	8	0	0.176 15	0
7	9	0	0.110 01	0
9	10	0.031 81	0.084 50	0
9	14	0.127 11	0.270 38	0
10	11	0.082 05	0.192 07	0
12	13	0.220 92	0.199 88	0
13	14	0.170 93	0.348 02	0

表 2 变压器参数

Table 2 Transformer parameters p.u.

首端节点	末端节点	电阻	电抗	变比
4	7	0	0.209 12	0.978
4	9	0	0.556 18	0.969
5	6	0	0.252 02	0.932

3.2 算例结果分析

利用遗传算法求解上述优化模型，攻击者可以得到使 SCED 成本最大的攻击策略。优化后的攻击策略如表 4、表 5 所示。

表 3 状态估计量测配置

Table 3 State estimation measurement configuration

节点（支路）	量测类型	量测值/p.u.	节点（支路）	量测类型	量测值/p.u.
1	1	1.060 0	4—9	4	0.154 6
2	2	0.183 0	5—2	4	−0.408 1
3	2	−0.942 0	5—4	4	0.600 6
7	2	0	5—6	4	0.458 9
8	2	0	6—13	4	0.183 4
10	2	−0.090 0	7—9	4	0.270 7
11	2	−0.035 0	11—6	4	−0.081 6
12	2	−0.061 0	12—13	4	0.018 8
14	2	−0.149 0	1—2	5	−0.174 8
2	3	0.352 3	2—3	5	0.059 4
3	3	0.087 6	4—2	5	0.021 3
7	3	0	4—7	5	−0.154 0
8	3	0.210 3	4—9	5	−0.026 4
10	3	−0.058 0	5—2	5	−0.019 3
11	3	−0.018 0	5—4	5	−0.100 6
12	3	−0.016 0	5—6	5	−0.208 4
14	3	−0.050 0	6—13	5	0.098 8
1—2	4	1.570 8	7—9	5	0.148 0
2—3	4	0.734 0	11—6	5	−0.086 4
4—2	4	−0.542 7	12—13	5	0.014 1
4—7	4	0.270 7			

表 4 交流部分攻击策略

Table 4 Attack strategy of AC part

节点（支路）	量测类型	量测值/p.u.	节点（支路）	量测类型	量测值/p.u.
1	1	1.060 0	2—3	4	0.819 4
2	2	0.181 5	4—2	4	−0.049 1
3	2	−1.285 4	4—7	4	0.144 4
4	2	−0.595 9	4—9	4	0.139 5
5	2	−0.093 1	5—2	4	−0.355 1
7	2	0	5—6	4	0.205 5
8	2	0	6—13	4	0.231 8
10	2	−0.097 4	7—9	4	0.331 5
11	2	−0.033 1	11—6	4	−0.103 8
12	2	−0.076 9	12—13	4	0.021 5
14	2	−0.157 6	1—2	5	−0.209 7
2	3	0.443 2	2—3	5	0.041 7
3	3	0.071 0	4—2	5	0.022 5
4	3	0.121 8	4—7	5	−0.158 3
5	3	0.308 1	4—9	5	−0.027 9
7	3	0	5—2	5	−0.020 9
8	3	0.270 3	5—6	5	−0.294 5
10	3	−0.070 9	6—13	5	0.108 9
11	3	−0.016 1	7—9	5	0.132 8
12	3	−0.013 1	11—6	5	−0.073 0
14	3	−0.058 6	12—13	5	0.014 9
1—2	4	1.726 1			

表 5　直流部分攻击策略

Table 5　Attack strategy of DC part　　p.u.

参数	整流侧	逆变侧
V^{m}	0.953 6	0.947 5
P_{ac}^{m}	0.298 8	−0.297 7
Q_{ac}^{m}	0.115 6	0.097 6
P_{dc}^{m}	0.300 7	−0.297 8
Q_{dc}^{m}	0.011 4	0.011 4

表 5 中,V^{m}为直流电压量测值;P_{ac}^{m}、Q_{ac}^{m}分别为交流侧换流母线有功、无功功率量测量;P_{dc}^{m}、Q_{dc}^{m}分别为直流有功、无功功率量测量。

利用该攻击方案进行 SCED,并与攻击前量测数据进行的 SCED 对比,得到的结果如表 6 所示。其中方案 1 为根据未受攻击的量测数据得到的 SCED 结果,方案 2 为根据优化模型得到的攻击方案所确定的 SCED 结果,方案 3 为随机选择节点 5 进行相角攻击时的 SCED 计算结果。

表 6　FDI 攻击策略优化结果

Table 6　FDI attack strategy optimization results　　MW

节点	发电机出力			切负荷量		
	方案 1	方案 2	方案 3	方案 1	方案 2	方案 3
1	172.70	211.80	205.80			
2	50.00	0	24.70	0	0	0
3	8.50	30.00	20.00	0	10.10	8.14
4				0	0	3.75
5				0	0	0
6	5.50	38.70	12.12	0	0	0
7						
8	20.00	20.00	7.55			
9				0	0	0
10				0	0	0
11				0	0	0
12				0	0	0
13				0	0	0
14				0	0	0

计算调度成本时,节点 1、2、3、6、8 上发电机的成本分别为 120、180、240、300、210 元/(MW·h);切负荷的成本为 600 元/(MW·h)。将发电机和负荷成本与发电机和负荷的调整功率代入目标函数,即可得到每个方案的调度成本。3 个方案的调度成本对比见图 4。方案 2 的攻击策略使得节点 3 与节点 6 的机组出力增加,且节点 3 的部分负荷被切除,导致 SCED 成本大大增加。方案 3 的攻击策略使得节点 1 和节点 3 的机组出力略有增加,节点 2 的机组出力略有降低,同时要切除部分负荷,使得方案 3 的 SCED 成本增加,但相较于方案 2,其 SCED 成本的增加量较小。这说明了方案 2 对攻击方案进行优化是有效的。

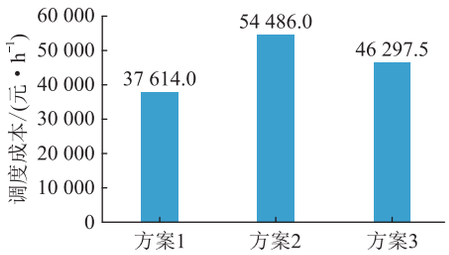

图 4　3 个方案的调度成本对比

Fig.4　Scheduling cost comparison of three schemes

当系统操作员根据方案 1 实施调度时,系统的真实运行状态与 SCED 计算结果基本保持一致;而根据方案 2 实施调度时,系统的真实运行状态与 SCED 计算结果可能有较大偏差,导致直流换流站换相失败。在实施调度方案之前,逆变侧换流母线的电压为 0.959 8 p.u.,由式(20)计算可得临界换相电压为 0.914 3 p.u.。在实施调度方案 2 之后,根据节点切负荷量和机组出力可得系统真实的运行状态,如表 7 所示。由表 7 可知,实施调度方案 2 之后,逆变侧换流母线节点的电压幅值为 0.907 9 p.u.,低于临界换相电压,因此可认为此时直流换流站发生换相失败。文中假设直流换流站发生换相失败导致直流闭锁,此时直流有功、无功输出为 0。

表 7　实施调度方案后的运行状态

Table 7　Operating status after implementing the scheduling scheme　　p.u.

节点	电压	相角	节点	电压	相角
1	0.966 8	0	8	0.987 0	−16.483 9
2	0.949 4	−5.967 5	9	0.932 1	−18.416 0
3	0.917 2	−14.144 3	10	0.931 7	−18.664 3
4	0.907 9	−12.826 9	11	0.950 1	−18.418 3
5	0.916 5	−10.985 6	12	0.968 4	−18.932 0
6	0.976 8	−17.907 8	13	0.951 2	−18.974 0
7	0.948 1	−16.486 4	14	0.920 1	−19.916 7

上述结果表明,当系统操作员根据优化模型所得的最优攻击策略进行调度时,会导致直流换流站换相失败。此时,在换流站发生换相失败而闭锁的前提下重新进行 SCED,得到的调度方案见表 8。此调度方案的成本为 74 040 元/h,明显高于根据最优攻击策略所得到的调度方案,说明考虑直流换流站换相失败时,其调度成本会进一步增加。同时,当直流换流站换相失败时,为保护直流换流站和维持交流系统的潮流稳定而调用的资源会使系统运行的成本进一步提高。

表 8 调度方案

Table 8 Scheduling scheme MW

节点	发电机出力	切负荷量	节点	发电机出力	切负荷量
1	172.0		8	20.0	
2	0	0	9		0
3	30.0	30.9	10		0
4		14.1	11		0
5		0	12		0
6	50.0	0	13		0
7			14		0

4 结语

文中建立的针对交直流混联电网的 FDI 攻击策略双层优化模型综合考虑系统操作员的动态行为与直流换流站换相失败的可能性，以 SCED 成本最大化为攻击策略优化目标，分析攻击过程中不良数据检测约束、篡改量测量的大小约束和调度时的约束，并采用遗传算法进行求解，以改进的 IEEE 14 节点系统为例验证了根据所提优化模型建立的攻击策略能够显著提高 SCED 的运行成本。当系统操作员根据此策略实施调度时，会引发直流换流站换相失败，进一步增加运行成本。文中在研究面向交直流混联电网的 FDI 攻击策略优化时，只考虑了攻击方如何实施攻击，未考虑防御方如何针对性制定防御措施。后续的工作将对换流母线电压低于临界换相电压时，发生换相失败的概率进行研究。柔直是直流输电发展的方向，后续工作还将对基于柔直的交直流混联系统的网络攻击方法进行研究。

参考文献：

[1] 单瑞卿，盛阳，苏盛，等. 考虑攻击方身份的电力监控系统网络安全风险分析[J]. 电力科学与技术学报，2022，37(5)：3-16.
SHAN Ruiqing，SHENG Yang，SU Sheng，et al. Risk analysis of power system cyber security considering identity of malicious adversaries[J]. Journal of Electric Power Science and Technology，2022，37(5)：3-16.

[2] LI J，SUN C W，SU Q Y. Analysis of cascading failures of power cyber-physical systems considering false data injection attacks [J]. Global Energy Interconnection，2021，4(2)：204-213.

[3] WU Y J，XU H，NI M. Defensive resource allocation method for improving survivability of communication and information system in CPPS against cyber-attacks[J]. Journal of Modern Power Systems and Clean Energy，2020，8(4)：750-759.

[4] LI H Y，HE X，ZHANG Y F，et al. Attack detection in cyber-physical systems using particle filter：an illustration on three-tank system[C]//2018 IEEE 8th Annual International Conference on CYBER Technology in Automation，Control，and Intelligent Systems (CYBER). Tianjin，China. IEEE，2019：504-509.

[5] CAI X P，WANG Q，TANG Y，et al. Review of cyber-attacks and defense research on cyber physical power system[C]// 2019 IEEE Sustainable Power and Energy Conference (iSPEC). Beijing，China. IEEE，2020：487-492.

[6] HOPKINS S，KALAIMANNAN E，JOHN C S. Cyber resilience using state estimation updates based on cyber attack matrix classification[C]//2020 IEEE Kansas Power and Energy Conference (KPEC). Manhattan，KS，USA. IEEE，2020：1-6.

[7] 童晓阳，王晓茹. 乌克兰停电事件引起的网络攻击与电网信息安全防范思考[J]. 电力系统自动化，2016，40(7)：144-148.
TONG Xiaoyang，WANG Xiaoru. Thoughts on network attacks caused by power outage in Ukraine and information security prevention of power grid[J]. Automation of Electric Power Systems，2016，40(7)：144-148.

[8] 邓松，张建堂，祝展望. 网络攻击下能源互联网数据容侵评估技术综述[J]. 电力信息与通信技术，2021，19(1)：11-19.
DENG Song，ZHANG Jiantang，ZHU Zhanwang. Overview of energy Internet data intrusion tolerance assessment technology under cyber attack[J]. Electric Power Information and Communication Technology，2021，19(1)：11-19.

[9] 钱胜，王琦，颜云松，等. 计及网络攻击影响的安全稳定控制系统风险评估方法[J]. 电力工程技术，2022，41(3)：14-21.
QIAN Sheng，WANG Qi，YAN Yunsong，et al. Risk assessment method of security and stability control system considering the impact of cyber attacks[J]. Electric Power Engineering Technology，2022，41(3)：14-21.

[10] 徐飞阳，薛安成，常乃超，等. 电力系统自动发电控制网络攻击与防御研究现状与展望[J]. 电力系统自动化，2021，45(3)：3-14.
XU Feiyang，XUE Ancheng，CHANG Naichao，et al. Research status and prospect of cyber attack and defense on automatic generation control in power system[J]. Automation of Electric Power Systems，2021，45(3)：3-14.

[11] TI B Z，WANG J X，LI G Y，et al. Operational risk-averse routing optimization for cyber-physical power systems[J]. CSEE Journal of Power and Energy Systems，2022，8(3)：801-811.

[12] DUO W L，ZHOU M C，ABUSORRAH A. A survey of cyber attacks on cyber physical systems：recent advances and challenges[J]. IEEE/CAA Journal of Automatica Sinica，2022，9(5)：784-800.

[13] LIU X L，LIU Y B，LIU J Y，et al. Optimal planning of AC-DC hybrid transmission and distributed energy resource system：review and prospects[J]. CSEE Journal of Power and Energy Systems，2019，5(3)：409-422.

[14] MEYER-HUEBNER N，SURIYAH M，LEIBFRIED T. Distributed optimal power flow in hybrid AC-DC grids[J]. IEEE Transactions on Power Systems，2019，34(4)：2937-2946.

[15] 王竞才，李琰，徐天奇. 基于扩展卡尔曼滤波的智能电网虚假数据检测[J]. 智慧电力，2022，50(3)：50-56.
WANG Jingcai，LI Yan，XU Tianqi. Detection of false data in smart grid based on extended Kalman filter[J]. Smart Power，

2022,50(3):50-56.

[16] YANG Q Y,YANG J,YU W,et al. On false data-injection attacks against power system state estimation: modeling and countermeasures[J]. IEEE Transactions on Parallel and Distributed Systems,2014,25(3):717-729.

[17] KEKATOS V,GIANNAKIS G B,BALDICK R. Grid topology identification using electricity prices[C]//2014 IEEE PES General Meeting | Conference & Exposition. National Harbor, MD,USA. IEEE,2014:1-5.

[18] ESMALIFALAK M,NGUYEN H,ZHENG R,et al. Stealth false data injection using independent component analysis in smart grid[C]//2011 IEEE International Conference on Smart Grid Communications (SmartGridComm). Brussels,Belgium. IEEE, 2011:244-248.

[19] LIU X,BAO Z,LU D,et al. Modeling of local false data injection attacks with reduced network information[J]. IEEE Transactions on Smart Grid,2015,6(4):1686-1696.

[20] 舒隽,郭志锋,韩冰. 电网虚假数据注入攻击的非线性分析模型[J]. 华北电力大学学报(自然科学版),2018,45(2)75-81.
SHU Jun,GUO Zhifeng,HAN Bing. Nonlinear analysis model of false data injection attack for power grid[J]. Journal of North China Electric Power University,2018,45(2)75-81.

[21] 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.
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.

[22] 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. Enlightenment from the Ukraine incident:preventing false data injection attacks against power grid[J]. Automation of Electric Power Systems,2016,40(7):149-151.

[23] 蔡星浦,王琦,郜伟,等. 基于多阶段博弈的电力 CPS 虚假数据注入攻击防御方法[J]. 电力建设,2019,40(5)48-54.
CAI Xingpu,WANG Qi,TAI Wei,et al. A multi-stage game based defense method against false data injection attack on cyber physical power system[J]. Electric Power Construction, 2019,40(5)48-54.

[24] 谢云云,严欣腾,桑梓,等. 面向交直流混联系统的虚假数据注入攻击方法[J]. 电力工程技术,2022,41(1):165-172.
XIE Yunyun,YAN Xinteng,SANG Zi,et al. False data injection attack method against AC-DC hybrid systems[J]. Electric Power Engineering Technology,2022,41(1):165-172.

[25] 樊磊. 网络攻击威胁下电力系统脆弱性分析模型与方法[D]. 北京:华北电力大学,2015.
FAN Lei. Vulnerability analysis model and method of power system under the threat of network attack[D]. Beijing:North China Electric Power University,2015.

作者简介:


谢云云

谢云云(1985),男,博士,副教授,研究方向为极端条件下电力系统运行与控制(E-mail:yunyun_xie@njust.edu.cn);

严欣腾(1996),男,硕士,从事极端条件下电力系统运行与控制工作;

燕子敖(1999),男,硕士在读,研究方向为极端条件下电力系统运行与控制。

Strategy optimization of false data injection attack on AC-DC hybrid systems

XIE Yunyun[1], YAN Xinteng[2], YAN Zi'ao[1], SANG Zi[3], YUAN Xiaoshu[3]

(1. School of Automation,Nanjing University of Technology,Nanjing 210094,China;
2. China Railway Shanghai Design Institute Group Co.,Ltd.,Shanghai 200072,China;
3. DEC Academy of Science and Technology Co.,Ltd.,Chengdu 611731,China)

Abstract: False data injection (FDI) attack is one of the attacks that can seriously affect the operation of power systems. Some studies have focused on the cyber-attack methods of AC-DC hybrid systems. However, few studies pay their efforts on the optimization of FDI attack on AC-DC hybrid systems. Therefore, an FDI attack strategy optimization method for AC-DC hybrid systems is proposed in the paper. Firstly, a two-layer optimization model with the objective of maximizing the loss of FDI attacks is established. In the upper model, the attacker launches FDI attack on the measuring system to find the optimal attack strategy to maximize the economic loss of the power system. The lower layer model calculates the maximum economic loss under a FDI attack with the objective of minimizing the generator output adjustment and load shedding, considering the security constraint of AD-DC hybrid system and the risk of commutate failure of DC converter station. Then, the two-layer optimization model is solved by the genetic algorithm to generate the optimal attack strategy. Finally, the improved IEEE 14-bus system is taken as an example to verify the effectiveness of the model. Simulation results show that the attack strategy optimized by the proposed method can effectively improve the cost of security constrained economic dispatch (SCED).

Keywords: AC-DC hybrid system; false data injection (FDI) attack; commutation failure; genetic algorithm; optimization model; security constrained economic dispatch (SCED)

(编辑 陆海霞)