DOI：10.13234/j.issn.2095-2805.2025.5.112　　**中图分类号**：TM40　　**文献标志码**：A

具有网络攻击防御力的DG变流器设计及其分布式控制

韦永军[1]，覃秋密[2]

(1.柳州铁道职业技术学院科技与图文信息处，柳州 545007；2.柳州铁道职业技术学院建筑技术学院，柳州 545007)

摘要：为了降低控制系统对通信网络的依赖性，直流微电网DC-MG(DC microgrid)通常采用分布式控制架构，然而由于缺乏全局信息，这种控制方式极易受到网络攻击，使得DC-MG存在较大安全隐患。网络攻击的种类较多，其中虚假数据注入攻击FDIA(false data injection attack)占比最高，其危害性也最大。基于此，针对FDIA造成DC-MG运行中断等不稳定问题，提出了1种基于前馈神经网络FNN(feedforward neural network)的DC-MG网络攻击检测与控制方法。该方法首先研究了FDIA造成控制系统不稳定的影响机理，建立了FDIA不稳定影响的数学模型；然后，利用FNN构建了智能估计器来监测DC-MG中分布式电源变换器的输出电流，并根据估计器的输出计算出FDIA的错误数据值；接着，针对错误数据的计算值，引入基于PI控制器的参考跟踪方法，以减少被攻击转换器中的错误数据，此外，所提方法还可消除所有高域不平衡攻击；最后，分别在MATLAB/Simulink和OPAL-RT环境下对所提方法进行了仿真和实验验证，仿真实验结果验证了所提方法的有效性。

关键词：直流微网；虚假数据注入攻击；前馈神经网络；网络攻击

Design and Distributed Control of DG Converter with Cyber-attack Defense Capability

WEI Yongjun[1], QIN Qiumi[2]

(1. Department of Science, Technology and Graphic Information, Liuzhou Railway Vocational Technical College, Liuzhou 545007, China; 2. School of Architecture and Technology, Liuzhou Railway Vocational Technical College, Liuzhou 545007, China)

Abstract: To reduce the dependence of a control system on the communication network, a DC microgrid (DC-MG) usually adopts the distributed control architecture. However, due to the lack of global information, this control mode is highly vulnerable to cyber-attacks, which leads to greater security risks in the DC-MG. There are many types of cyber-attacks, among which the false data injection attacks (FDIA) account for the highest proportion and pose the biggest danger. On this basis, aimed at the instability problems such as interruption of DC-MG operation caused by FDIA, a DC-MG cyber-attack detection and control method based on feedforward neural network (FNN) is proposed. First, the influence mechanism of FDIA causing the instability of the control system is studied, and a mathematical model of instability caused by FDIA is established. Second, an intelligent estimator is constructed by using FNN to monitor the output current from a distributed power converter in the DC-MG, and the error data values of FDIA are calculated according to the output from the estimator. Third, aimed at the calculated values of error data, a reference tracking method based on a PI controller is introduced to reduce the error data in the attacked converter. In addition, the proposed method can eliminate all the high-domain unba-lanced attacks. Finally, the proposed method was simulated and verified by experiments carried out in MATLAB/Simulink and OPAL-RT, respectively, and results proved its effectiveness.

收稿日期：2022-07-29；**修回日期**：2022-11-13，2022-11-29；
录用日期：2022-12-28；**网络首发日期**：2023-02-23
基金项目：广西高校中青年教师基础能力提升项目(2020KY44016)
This work is supported by Basic Ability Improvement Project of Young and Middle-aged Teachers in Guangxi Universities under the grant 2020KY44016

Keywords: DC microgrid (DC-MG); false data injection attack (FDIA); feedforward neural network (FNN); cyber-attack

与交流微电网相比，直流微电网 DC-MG(DC microgrid)具有更高的效率和更低的控制复杂度，它通过通信网络可实现电源间的协调控制，可进一步提高运行效率[1]。DC-MG 存在 2 种典型的通信拓扑：集中式和分布式[2]。集中式通信拓扑便于实现，且结构简单，但受单点故障和控制延迟等因素影响较大，因此，这种方式可靠性较差。而分布式通信拓扑由于只在相邻物理单元之间共享信息，对通信网络依赖性较小，其可靠性和灵活性较高。另外，对于有界通信延迟和通信网络故障，基于分布式通信拓扑的控制系统鲁棒性更好[3-4]。然而，当 DC-MG 采用协同分布式控制策略运行时，由于只有相邻电源交换信息，缺少系统全局信息，故协同型直流微电网极易受到网络攻击，这也是 DC-MG 在正常运行中面临的关键难题之一[5-9]。网络攻击是利用人为设计的特殊计算机程序或病毒及其他手段破坏国标计算机网络系统以降低其使用功效的行为，其种类多种多样，如拒绝服务 DoS(denial of service)攻击、重放攻击和假数据攻击 FDIA(false data injection attack)，其中，FDIA 在网络攻击中占比较高，故其危害性最大。FDIA 属于隐形攻击，其通过欺骗控制应用程序，使系统运行者无法获取系统的在线攻击信息，可在不受任何干扰地情况下将虚假数据注入系统，当攻击者侵入控制系统后，以不平衡的方式增加被攻击单元的输出大小，导致直流微电网运行崩溃。

针对上述问题，国内外学者开展了一定研究，其中基于协同一致性原理的直流微电网分布式控制策略得到了广泛关注。在 DC-MG 中协同控制的目标是利用本地和相邻单元的数据信息来调节平均电压及按比例分配电流[8]。为了保护微电网系统不受此类事件的影响，本文主要针对 FDIA 对 DC-MG 的影响展开研究[10]，提出了 1 种监测协同型 DC-MG 中虚假数据值及消除 DC-MG 中 FDIA 的方法，可较高精度的识别虚假数据的攻击，以保障 DC-MG 的安全稳定运行。所提方法首先设计了 1 种基于前馈神经网络 FNN(feedforward neural network)的估计器来监测连接分布式能源 DER (distributed energy resource)的变流器输出电流，并根据估计器的输出计算出 FDIA 和错误数据的值；然后，针对错误数据的计算值，引入基于 PI 控制器的参考跟踪方法，以减少被攻击变流器中的错误数据。

1　FDIA 对直流微电网的影响机理建模

1.1　前馈神经网络

FNN 由具有多个输入的输入层、1 个或多个隐含层和 1 个输出层组成[11]。在前馈结构中，每一层都由大量神经元构成，数据从一层的神经元传播到另一层。图 1 为前馈神经网络的一般结构图[12]。图中，$x_i(i=1, 2, \cdots, k)$和 y 分别为神经网络的第 i 个输入和输出。

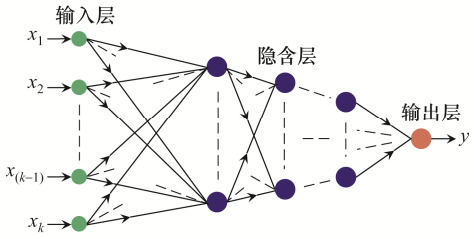


图 1　前馈神经网络的一般结构

Fig. 1 Common structure of feedforward neural network

将输入层和输出层分别作为神经网络的第一层和最后一层，图 2 为第 l 层第 j 个神经元的结构。图中：M_{l-1} 为第 l 层神经元数量；b_j^l 为第 l 层第 j 个神经元的偏置权值；$f(\cdot)$ 为神经元的激活函数；ω_{rj}^l 为连接的权重；α_j^l 为第 l 层的第 j 个神经元输出[13]，可表示为

$$\alpha_j^l = f\left(\left(\sum_{i=1}^{M_{l-1}} \alpha_i^{l-1} \cdot \omega_{rj}^l\right) + b_j^l\right) \tag{1}$$

FNN 的实现包含 2 个步骤：

(1)离线训练神经网络以建立 1 个精细的调谐神经网络[14]；

(2)训练好的前馈神经网络用于监测和估计变换器的输出电流。

其中，FNN 的隐含层的输出可表示为

$$\bar{y}=f_{\text{out}}(f_{\text{hid}}(\boldsymbol{X}\boldsymbol{W}^{\text{hid}}+\boldsymbol{b}^{\text{hid}})\boldsymbol{W}^{\text{out}}+b^{\text{out}}) \tag{2}$$

式中：f_{hid} 和 f_{out} 分别为隐含层和输出层神经元的激活函数；$\bar{y}$ 为前馈神经网络的估计输出；$\boldsymbol{X}$ 为有 k 个输入的神经网络的输入向量，$\boldsymbol{X}=f(x_1,x_2,\cdots,x_{k-1},x_k)$；$b^{\text{out}}$ 为输出层神经元的偏置权值；$\boldsymbol{W}^{\text{hid}}$、$\boldsymbol{W}^{\text{out}}$ 和 $\boldsymbol{b}^{\text{hid}}$ 分别为隐含层的权矩阵、输出层的权向量和隐含层的偏差向量。前馈神经网络离线训练的目的是寻找 $\boldsymbol{W}^{\text{hid}}$、$\boldsymbol{W}^{\text{out}}$ 和 $\boldsymbol{b}^{\text{hid}}$ 的最优值；b^{out} 为 1 个微调的神经网络来正确地估计输出。

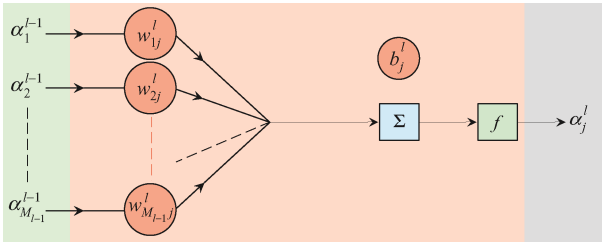


图 2 第 *l* 层第 *j* 个神经元的结构

Fig. 2 Structure of *j*th neuron in *l*th layer

1.2 协同型直流微电网的信息物理模型

图 3 为含 M 个分布式发电单元 DG(distributed generation)直流微电网的信息物理模型。直流微电网通常由 M 个分布式发电单元组成，每个发电单元由 1 个直流电源，通过 DC-DC 变流器连接到直流微电网母线上，所有变流器的额定功率都是相等的。每个变流器根据本地主控制器和从控制器设置的参考电压来维持输出电压。

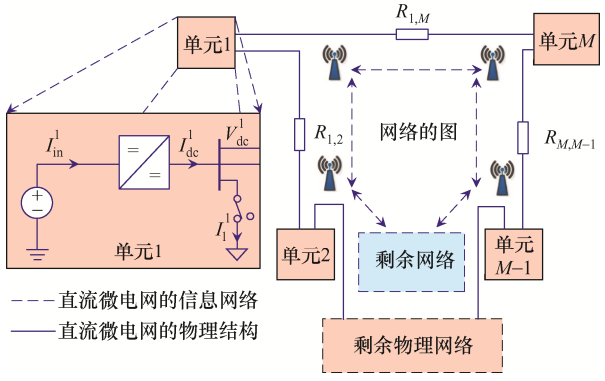


图 3 含 *M* 个分布式电源直流微电网的信息物理模型

Fig. 3 Information physical model of DC microgrid with *M* DGs

图 4 为分布式电源的协同控制示意图，图中：$V_{\text{dc}_{\text{ref}}}$ 和 $I_{\text{dc}_{\text{ref}}}$ 分别为所有单元的电压和电流的全局参考值；$V^i_{\text{dc}_{\text{ref}}}$ 为每个变流器的输出电压；$\bar{V}^i_{\text{dc}}$ 为第 i 个单元估计的平均电压。在全局电压基准中增加 2 个电压项，形成本地电压参考值，以维持 $V^i_{\text{dc}_{\text{ref}}}=V_{\text{dc}_{\text{ref}}}+\Delta V_v+\Delta V_i$；$I_{\text{dc}_{\text{ref}}}$=0 表示各单元之间按比例分配负载电流；控制系统根据动态一致性更新电压和电流，即

$$\bar{V}^i_{\text{dc}}(t)=V^i_{\text{dc}}(t)+\int_0^t\sum_{j\in M_i}a_{ij}[\bar{V}^j_{\text{dc}}(\tau)-\bar{V}^i_{\text{dc}}(\tau)]\text{d}\tau \tag{3}$$

$$\bar{I}^i_{\text{out}}(k)=\sum_{j\in M_i}c_i a_{ij}\left[\frac{I^j_{\text{dc}}(k)}{I^j_{\max}}-\frac{I^i_{\text{dc}}(k)}{I^i_{\max}}\right] \tag{4}$$

式中：M_i 为第 i 个单位的相邻集合；c_i 和 I^i_{dc} 分别为第 i 个单元的耦合增益和测量的第 i 个变换器的输出电流；$I^i_{\max}$ 为第 i 个转换器允许的最大输出电流；a_{ij} 为通信邻接矩阵中的元素，若第 i 个单元与第 j 个单元间存在通信连接，则 $a_{ij}=1$，否则为 0；τ 为时间积分变量。

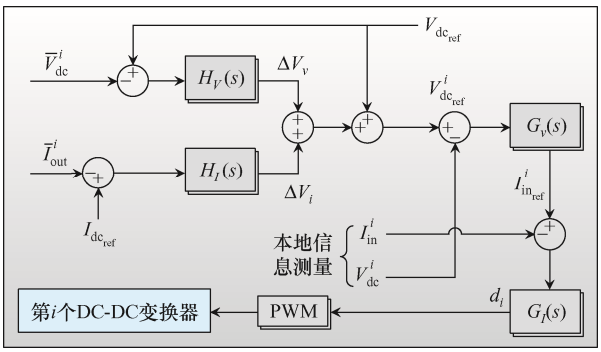


图 4 分布式电源的协同控制示意

Fig. 4 Schematic of cooperative control of DGs

通过分布式一致性算法，对于连通良好的网络图，直流微电网的协同控制目标收敛条件为

$$\begin{cases}\lim\limits_{k\to\infty}\bar{V}^i_{\text{dc}}(k)=V_{\text{dc}_{\text{ref}}} & \forall i\in M\\ \lim\limits_{k\to\infty}\bar{I}^i_{\text{out}}(k)=0 & \forall i\in M\end{cases} \tag{5}$$

1.3 FDIA 对直流微电网的影响模型

当直流微电网受到 FDIA 攻击时，直流微电网的控制目标则不会遵循式(5)，但一些攻击可以通过更复杂的编程来遵循式(5)欺骗直流微电网的运行调度者[15]。本文针对现有的测量方法，重点研究

了 FDIA 攻击的检测和抑制方法。对第 i 个单元中电流传感器的攻击可表示为

$$I_{\mathrm{a}}^{i}=I_{\mathrm{dc}}^{i}+\kappa_i I_{\mathrm{f}}^{i} \tag{6}$$

式中：I_{a}^{i} 为报告给控制器的第 i 单元的输出电流值；I_{dc}^{i} 为第 i 单元输出电流的实际值；I_{f}^{i} 为攻击者注入系统的虚假数据；κ_i 为 1 个二进制参数，κ_i=1 表示存在攻击元素，反之亦然。因此，通信网络中的 FDIA 可表示为

$$I_{\mathrm{a}}^{ij}=I_{\mathrm{dc}}^{j}+\kappa_i I_{\mathrm{f}}^{i} \qquad \forall j\in M_i \tag{7}$$

式中，I_{a}^{ij} 为第 i 个单元的输出电流值，发送到第 j 个单元。FDIA 是指将错误数据注入传感器和通信网络，在直流微电网中，FDIA 攻击类似于 1 种负载变化，它满足了协同控制的目标，即电流分配和平均调压[16]。

2　计及 FDIA 的分布式一致性控制方法

由于 FDIA 攻击也满足直流微电网的协同控制目标收敛条件，即式(5)，这使得仅通过监测协同控制信号很难识别是否存在攻击，基于此，所提分布式一致性控制目标是检测和减轻变流器输出电流测量中的 FDIA[17-19]。该控制策略基于 PI 控制器对各变流器输出电流的参考值进行跟踪，有效减少系统内的错误数据。此外，本文还设计了 1 个本地估计器，利用人工神经网络对变流器的输出电流进行估计，并给出 PI 控制器的参考值，PI 控制器的输出被增加到转换器的输出电流中。

图 5 为基于 PI 的参考跟踪方法在第 i 发电单元中的运用图。可知，如果第 i 单元中没有攻击缓解器和 PI 控制器，则本地控制器中使用并发送给相邻变流器的输出电流值为

$$I_{\mathrm{M}}^{i}(k)=I_{\mathrm{a}}^{i}(k)=I_{\mathrm{dc}}^{i}(k)+\kappa_i I_{\mathrm{f}}^{i} \tag{8}$$

式中，I_{M}^{i} 为第 i 单元变流器输出电流的总值。当第 i 个单元中存在攻击缓解层时，I_{M}^{i} 可表示为

$$I_{\mathrm{M}}^{i}(k)=I_{\mathrm{dc}}^{i}(k)+\kappa_i I_{\mathrm{f}}^{i}+\beta_i \tag{9}$$

式中，β_i 为 PI 控制器的第 i 单元输出。

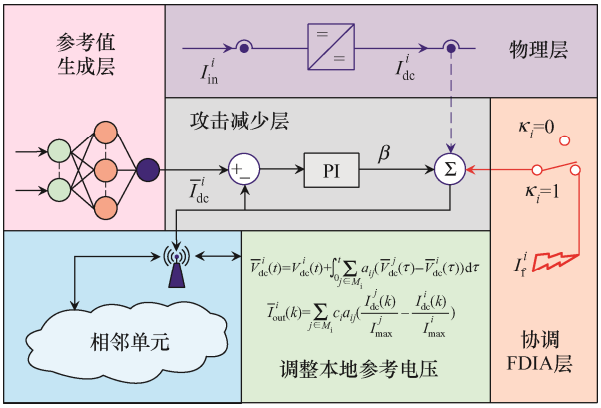


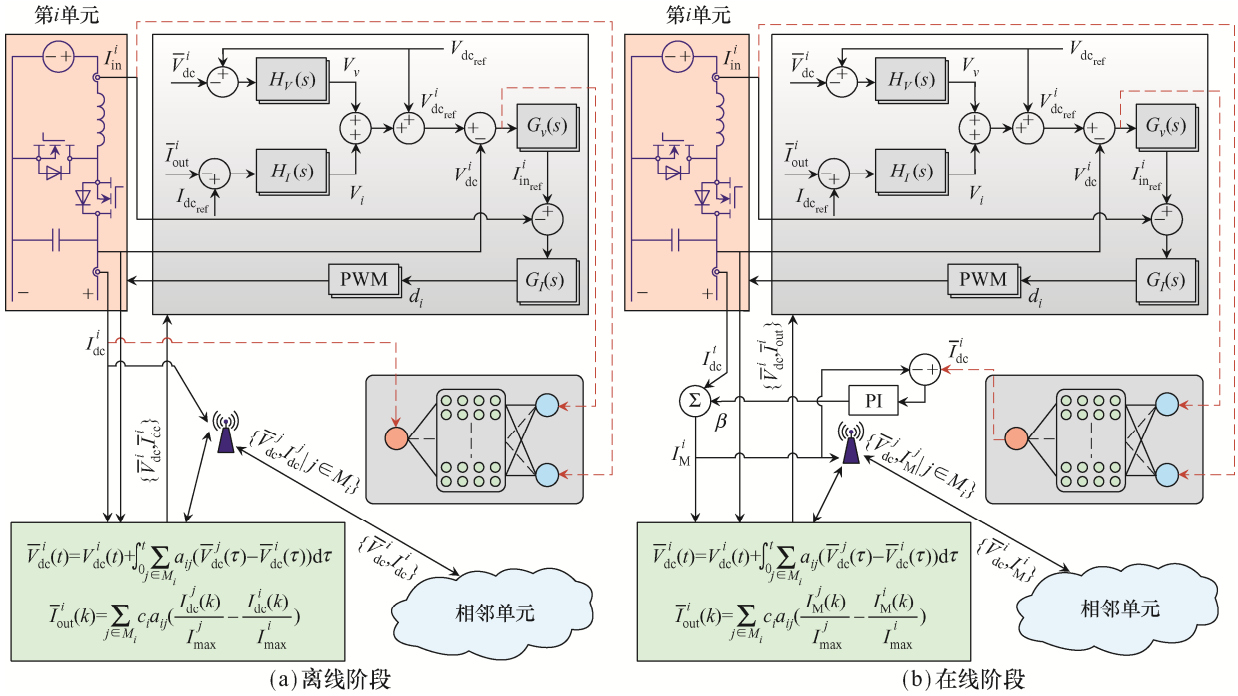
图 5　基于 PI 的参考跟踪方法在第 *i* 发电单元中的运用

Fig. 5 Application of reference tracking method based on PI in *i*th power generation cell

即使存在攻击的情况下 PI 控制器也可用来跟踪 I_{dc}^{i} 和 I_{M}^{i}。$\bar{I}_{\mathrm{dc}}^{i}$ 为第 i 单元输出电流的估计值，用于攻击缓解层。β_i 可以写成

$$\beta_i=-\kappa_i I_{\mathrm{f}}^{i} \tag{10}$$

PI 控制器试图控制增加变流器的输出电流总值，以消除 FDIA 攻击对发电单元的影响。根据式(10)，β_i 是本地监控第 i 个单元的合适指标。如果 β_i 不为 0，表明第 i 个单元受到攻击；如果第 i 个单元没有受到攻击，则 β_i=0。本文选择 I_{in}^{i} 和 $V_{\mathrm{dc_{ref}}}^{i}-V_{\mathrm{dc}}^{i}$ 作为神经网络的输入用于估计。在神经网络在线运行之前，需要对神经网络进行训练，以确定相邻神经元之间的最优连接权值，此外，还要对神经元的偏置权值进行训练，以将神经网络训练好。为了较好地实现网络训练，需要收集 1 组神经网络的数据输入和数据输出，用于训练阶段。其中，训练是离线实现的。图 6 为离线训练神经网络准备在每个机组在线实现，以估计该机组的输出电流。



(a) 离线阶段 (b) 在线阶段

图 6 直流微电网第 i 发电单元中神经网络控制方框图

Fig. 6 Control block diagram of neural network in ith power generation cell of DC microgrid

3 仿真与实验验证

3.1 仿真验证

为了验证所提方法的有效性，在 Simulink 仿真平台进行了验证。仿真测试系统结构如图 3 所示，其中，M=4，测试系统相关参数见表 1。

表 1 直流微网相关参数

Tab. 1 Related parameters of DC microgrid

参数	数值	参数	数值
R_{12}/Ω	1.8	L_1、L_2/mH	5
R_{23}/Ω	2.3	C_1、C_2/mF	50
R_{34}/Ω	2.1	Δt/ms	0.1
R_{14}/Ω	1.3	V_{in}^3、V_{in}^4/V	270
$V_{\text{dc}_{\text{ref}}}$/V	315	L_3、L_4/mH	5
V_{in}^1、V_{in}^2/V	270	C_3、C_4/mF	50

测试算例采用 1 个含 10 个神经元隐含层的前馈神经网络对变流器的输出电流进行估计。为了避免神经网络复杂化，本文采用的神经网络为单隐含层，该网络有 2 个输入端和 1 个输出端，且输入层的神经元数为 2 个，输出层的神经元数等于神经网络的输出数。神经网络的输出为输出电流的估计值。为了收集数据来训练神经网络，当仿真模型运行时，在给定的持续时间(20 s)内，每 0.1 ms 收集一次数据，因此，收集的一组数据由 200 000 个 $\{I_{\text{in}}^1,(V_{\text{dc}_{\text{ref}}}^1-V_{\text{dc}}^1)\}$ 样本组成，其作为神经网络的输入。此外，选择 200 000 个样本 $\{I_{\text{in}}^1\}$ 作为用于训练阶段的神经网络输出。在收集数据的选定时间内，仿真过程中考虑了 14 次负载变化，其中 11 个发生在 1 号机组。当收集数据以获得更精确的基于神经网络的估计器时，这些负载变化被认为是映射变流器的动态特性。此外，经神经网络隐含层的激活函数 $f_1(x)=\dfrac{2}{1+\mathrm{e}^{-2x}}-1$ 和输出层激活函数 $f_2(x)=x$ 分别为 sigmoid 和线性激活函数[20]。另外，DC-MG 的母线参考电压为 315 V。

3.1.1 FDIA 攻击下注入虚假数据的验证

1 号发电单元在 t=0.5 s 发生负载变化，1 s 后开始向 1 号发电单元注入值为 2 的错误数据，并进行 FDIA 协同攻击。图 7 为变换器的输出电流变化，图 8 为协调攻击时所有发电单元的直流电压。由图 7 和图 8 可知，FDIA 攻击迅速从被攻击发电单元中移除。

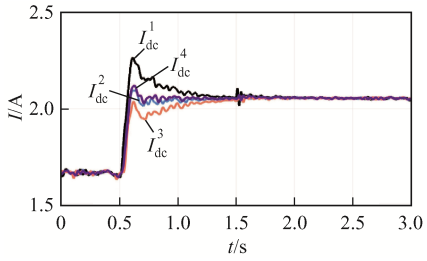


图 7　FDIA 攻击中所有发电单元的直流输出电流

Fig. 7 DC output current from all power generation cells under FDIA

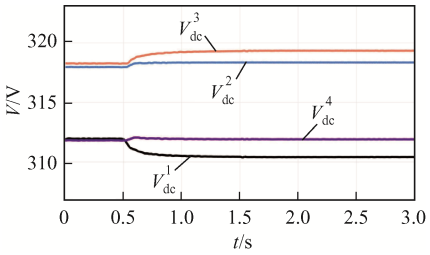


图 8　FDIA 攻击时各单元的直流电压

Fig. 8 DC voltage of each cell under FDIA

图 9 为所有发电单元的错误数据估计值，本文方法根据结果对所有单元的错误数据进行了精确估计。如图所示，$-\beta_i$ 对于 i=2，3，4 均为 0，但在 t=1.5 s 时，$-\beta_i$ 开始增加，i 达到 2，这意味着被攻击的发电单元被一个值为 2 的错误数据所攻击。

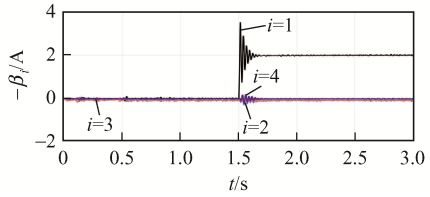


图 9　估计出的所有发电单元的注入虚假数据

Fig. 9 Estimated false data injection for all power generation cells

图 10 为不同比例系数 K_p 值下被攻击发电单元的假数据估计值。可知，当 K_p=60 时，系统存在明显的振荡现象，假数据估计存在较大的超调量和持续波动；而随着 K_p 值逐渐增大至 100、250 和 400，估计结果的动态响应变得更加平滑，振荡频率和幅度明显减小，系统的稳定性显著提升。这表明比例系数对估计器的动态性能具有显著影响，较大的 K_p 值有助于加快估计误差的收敛速度，提高对伪数据注入攻击的辨识精度和抑制能力，但也需注意参数过大可能引入响应延迟或系统刚性。

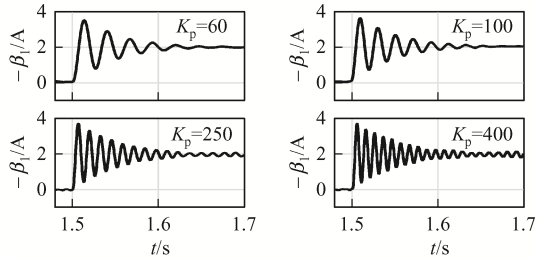


图 10　不同 K_p 下被攻击单元中注入假数据的估计值

Fig. 10 Estimated false data injection in attacked cells under different values of K_p

3.1.2　大规模 FDIA 攻击下所提方法的有效性验证

本文还验证了不同时间下多个发电单元受到 FDIA 攻击，以进一步验证所提方法的有效性。即在 t=0.5、1.5、2.5、3.5 s 时，分别将+1、−0.5、+1 和+0.5 的假数据注入发电单元 1、发电单元 2、发电单元 3 和发电单元 4。图 11 为直流微电网中 DC-DC 变流器的输出电流。可以看出，本文提出方法即使在所有单位都受到攻击的情况下，也可消除大规模 FDIA。

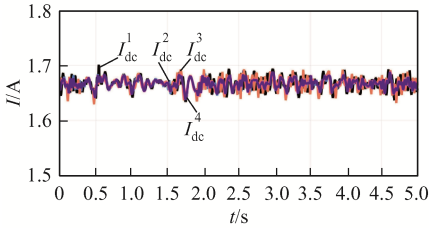


图 11　大范围 FDIA 攻击时各机组的直流输出电流

Fig. 11 DC output current from each unit under large-scale FDIA

图 12 为所提策略对假数据的估计值。可以看出，所提出的方法能够成功地检测出被攻击发电单位，且能够可靠地估计出错误数据的值。

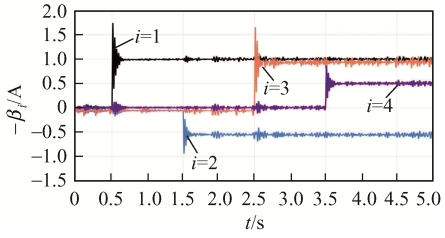


图 12　估计所有单元的假注入数据

Fig. 12 Estimated false data injection for all cells

图 13 为不同比例系数 K_p 下假数据的估计值。当 K_p 较小时(如 60)，估计结果出现较明显的振荡与超调，且假数据在多个单元之间的传播具有较强的耦合性，导致干扰持续时间较长；随着 K_p 增大至 250 或 400，估计信号在干扰发生初期迅速趋于平稳，表明系统具备较好的扰动抑制和局部化响应能力。此外，攻击事件在各个单元上的响应差异也反映出系统对假数据注入具有一定的空间选择性，说明合理调整 K_p 有助于增强定位精度和稳态估计性能。

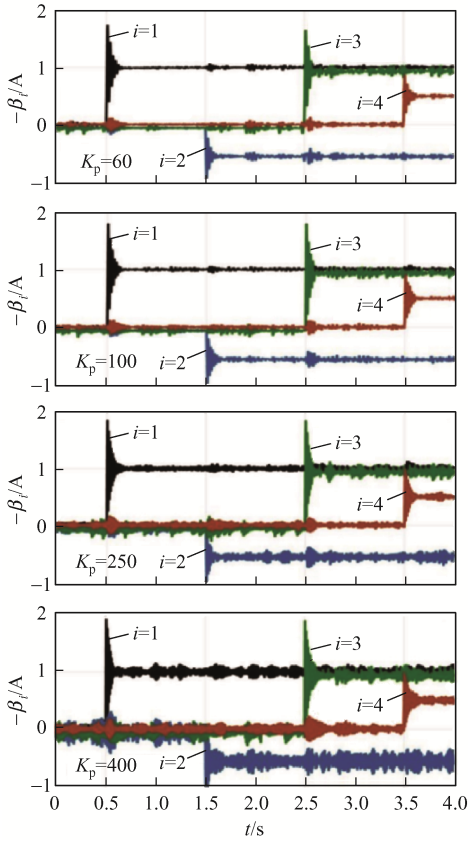


图 13 不同 K_p 下各发电单元假注入数据的估计值

Fig. 13 Estimated false data injection for each power generation cell under different values of K_p

3.2 实时仿真验证

为了进一步验证所提方法的有效性，本文基于 OPAL-RT 对所提方法进行了实时仿真分析，以评估所提方法的有效性。实时仿真系统由 OPAL-RT、电脑和路由器组成，其中，OPAL-RT 的运行软件为 MATLAB 集成的 RT-LAB，通过 RT-LAB 打开 MATLAB/Simulink 环境，生成模型的 C 语言代码，该代码可在实时系统上运行，仿真系统的采样时间为 5×10^{-5} s。实时仿真系统包含 3 个子系统，即主系统、从系统和控制系统，其中，主系统是模拟各发电单元的物理模型，从系统则是控制模型的计算部分。本案例考虑所有发电单元同时受到假数据值的协同攻击，其中，发电单元 1、2、3、4 分别注入+80、+60、+40、+20 的假数据，图 14(a)和(b)分别为直流微电网的电流和电压。可以看出，实时仿真结果表明所提方法消除了不平衡攻击的影响。

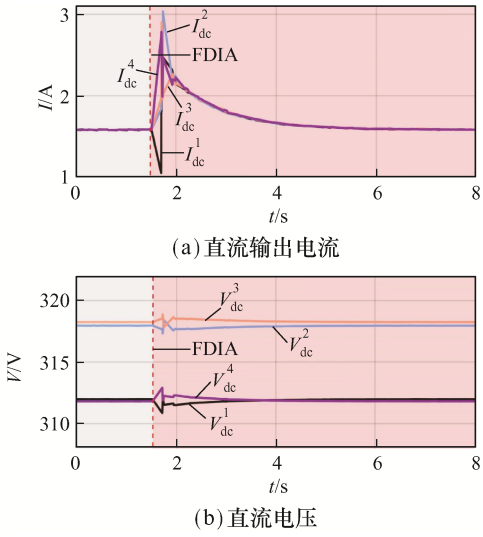


图 14 实时仿真中各发电单元的直流电流值和直流电压值

Fig. 14 Values of DC current and DC voltage of each power generation cell in real-time simulation

图 15 为不同 i 值下 $-\beta_i$ 的变化情况。图 15 中给出了实时仿真中各单元注入假数据估计值 $-\beta_i$ 的时间响应，虚线处为攻击开始时刻。攻击发生后，各曲线均出现突变并在极短时间内衰减至稳定，这说明估计器能够快速收敛并保持输出恒定。稳态幅值满足 $-\beta_1>-\beta_2>-\beta_3>-\beta_4$，反映出各单元受到

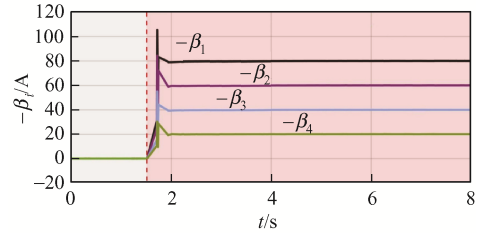


图 15 实时仿真中所有单元的假注入数据的估计

Fig. 15 Estimation of false data injection for all cells in real-time simulation

的假数据强度或敏感性不同，所提算法对后续噪声和扰动具有较强鲁棒性。

4　结语

本文提出了 1 种基于前馈神经网络的直流微电网抵御 FDIA 攻击的协同控制策略。该方法首先在各发电单元中使用神经网络对各变流器的输出电流进行估计，并根据估计值基于 PI 控制器来消除被攻击单元的攻击；所提方法属于 1 种分散的方法，只需要在相邻单元间交换少量数据。此外，该方法在任何单元受到攻击时均可确定错误数据的值。最后，仿真与实验结果表明，即使发生大规模所有单元注入虚假数据攻击时，所提方法也能成功地检测并消除直流微网中所有单元受到的攻击。

参考文献：

[1] 葛磊蛟, 李元良, 汪宇倩. 智能配电网态势感知实现效果综合评估模型[J]. 天津大学学报(自然科学与工程技术版), 2020, 53(11): 1101-1111.
Ge Leijiao, Li Yuanliang, Wang Yuqian. Comprehensive evaluation model for situational awareness effects of a smart distribution network [J]. Journal of Tianjin University (Science and Technology), 2020, 53(11): 1101-1111. (in Chinese)

[2] 张冀川, 陈蕾, 张明宇, 等. 配电物联网智能终端的概念及应用[J]. 高电压技术, 2019, 45(6): 1729-1736.
Zhang Jichuan, Chen Lei, Zhang Mingyu, et al. Conception and application of smart terminal for distribution internet of things [J]. High Voltage Engineering, 2019, 45(6): 1729-1736. (in Chinese)

[3] 吴在军, 徐俊俊, 余星火, 等. 主动配电网状态估计技术评述[J]. 电力系统自动化, 2017, 41(13): 182-191.
Wu Zaijun, Xu Junjun, Yu Xinghuo, et al. Review on state estimation technique of active distribution network [J]. Automation of Electric Power Systems, 2017, 41(13): 182-191. (in Chinese)

[4] 徐俊俊, 吴在军, 胡秦然, 等. 考虑多类型分布式电源和负荷不确定性的主动配电网区间状态估计[J]. 中国电机工程学报, 2018, 38(11): 3255-3266.
Xu Junjun, Wu Zaijun, Hu Qinran, et al. Interval state estimation for active distribution networks considering uncertainties of multiple types of DGs and loads [J]. Proceedings of the CSEE, 2018, 38(11): 3255-3266. (in Chinese)

[5] 杨勇, 李继红, 周自强, 等. 智能配电柔性多状态开关技术、装备及示范应用[J]. 高电压技术, 2020, 46(4): 1105-1113.
Yang Yong, Li Jihong, Zhou Ziqiang, et al. Technology, equipment and demonstration application of flexible multi-state switch in intelligent distribution network [J]. High Voltage Engineering, 2020, 46(4): 1105-1113. (in Chinese)

[6] Zhao Junbo, Mili L, Wang Meng. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures [J]. IEEE Transactions on Power Systems, 2018, 33(5): 4868-4877.

[7] Che Liang, Liu Xuan, Li Zuyi. Fast screening of high-risk lines under false data injection attacks [J]. IEEE Transactions on Smart Grid, 2019, 10(4): 4003-4014.

[8] 赵丽莉, 刘忠喜, 孙国强, 等. 基于非线性状态估计的虚假数据注入攻击代价分析[J]. 电力系统保护与控制, 2019, 47(19): 38-45.
Zhao Lili, Liu Zhongxi, Sun Guoqiang, et al. Cost analysis of the false data injection attack based on nonlinear state estimation [J]. Power System Protection and Control, 2019, 47(19): 38-45. (in Chinese)

[9] Liang Gaoqi, Zhao Junhua, Luo Fengji, et al. A review of false data injection attacks against modern power systems [J]. IEEE Transactions on Smart Grid, 2017, 8(4): 1630-1638.

[10] 丘恒越, 张桂东, 陈思哲. 基于准 Z 源的低电容电压应力高增益 DC-DC 变换器. 电源学报. 2024, 22(6): 1-12.
Qiu Hengyue, Zhang Guidong, Chen Sizhe. High-gain DC-DC converter with low voltage stress of capacitor based on quasi-Z-source [J]. Journal of Power Supply. 2024, 22(6): 1-12. (in Chinese)

[11] Zhang Yichi, Xiang Yingmeng, Wang Lingfeng. Power system reliability assessment incorporating cyber-attacks against wind farm energy management systems [J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2343-2357.

[12] Zhao Junbo, Zhang Gexiang, Dong Zhaoyang, et al. Forecasting-aided imperfect false data injection attacks against power system nonlinear state estimation [J]. IEEE Transactions on Smart Grid, 2015, 7(1): 6-8.

[13] Teixeira A, Dán G, Sandberg H, et al. A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator [J]. IFAC Proceedings Volumes, 2011, 44(1): 11271-11277.

[14] Teixeira A, Dán G, Sandberg H, et al. Security of smart distribution grids: Data integrity attacks on integrated volt/VAR control and countermeasures [C]// 2014 American Control Conference. Portland, OR, USA, 2014: 4372-4378.

[15] 徐海亮, 张伟杰, 林鸿彬. 一种提高并网逆变器无源性的阻抗重塑方法. 电源学报. 2025, 23(3): 269-279.
Xu Hailiang, Zhang Weijie, Lin Hongbin. Impedance remodeling method for improving passivity of grid-connected inverters [J]. Journal of Power Supply. 2025, 23(3): 269-279. (in Chinese)

[16] Hug G, Giampapa J A. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks [J]. IEEE Transactions on Smart Grid, 2012, 3(3): 1362-1370.

[17] Kang J W, Joo I Y, Choi D H. False data injection attacks on contingency analysis: Attack strategies and impact assessment [J]. IEEE Access, 2018, 6: 8841-8851.

[18] Moslemi R, Mesbahi A, Mohammadpour Velni J. Design of robust profitable false data injection attacks in multi-settlement electricity markets [J]. IET Generation, Transmission & Distribution, 2018, 12(6): 1263-1270.

[19] 李俊辉, 曾君, 樊淼嘉, 等. 基于改进 CRPS 和 QR-CNN-LSTM-SA 模型的短期光伏功率非参数概率预测 [J/OL]. 电源学报, 1-11. (2025-05-18)[2025-06-26]. http://kns.cnki.net/kcms/detail/12.1420.tm.20250515.1454.006.html.
Li Junhui, Zeng Jun, Fan Miaojia, et al. Non-parametric probability prediction of short-term photovoltaic power based on improved CRPS and QR-CNN-LSTM-SA models [J/OL]. Journal of Power Supply, 1-11. (2025-05-18) [2025-06-26]. http://kns.cnki.net/kcms/detail/12.1420.tm.20250515.1454.006.html. (in Chinese)

[20] Deng Ruilong, Liang Hao. False data injection attacks with limited susceptance information and new countermeasures in smart grid [J]. IEEE Transactions on Industrial Informatics, 2018, 15(3): 1619-1628.



韦永军

作者简介：

韦永军(1983—)，男，通信作者，硕士，高级工程师。研究方向：信息安全及云计算。E-mail：ccnn1234562021@126.com。

覃秋密(1984—)，女，本科，讲师。研究方向：教学管理。E-mail：254011998@qq.com。

(责任编辑：郭凯凯)