文章编号：2095-4980(2025)07-0685-07

考虑广义FDI攻击的配电云主站韧性协同控制

刘　昊[1]，张　凯[2]，郭祥富[1]，胡誉蓉[1]，贺　翔[1]，赵　健[1]

(1.国网河南省电力公司 电力科学研究院，河南 郑州 450052；2.国网河南省电力公司，河南 郑州 450052)

摘　要：随着"双碳"战略的推进，配电网由传统单向辐射供给向多分布式电源参与的有源配电网转变。配电云主站采集各分布式电源并实现多源协同依赖于稀疏的通信网络，因此受到虚假数据注入(FDI)恶意攻击的威胁。为应对具备高频高阶导数无界的广义FDI威胁，提出一种面向有源配电网的完全分布式二次韧性控制策略。借助高阶积分压制系数，有限阶导数有界的控制通道FDI得到抑制。通过Lyapunov法证明，所提出的防御策略可实现频率调节的均匀最终有界(UUB)收敛，并在改进型IEEE 9-bus系统有源配电网上进行了验证。

关键词：有源配电网；分布式控制；韧性控制；虚假数据注入；配电云主站

中图分类号：TM762；TN711　　**文献标志码：**A　　**DOI：**10.11805/TKYDA2024591

Resilient coordinated control of distribution cloud master station considering generalized FDI attacks

LIU Hao[1]，ZHANG Kai[2]，GUO Xiangfu[2]，HU Yurong[1]，HE Xiang[1]，ZHAO Jian[1]

(1.Electric Power Research Institute，State Grid Henan Electric Power Company，Zhengzhou Henan 450052，China；
2.State Grid Henan Electric Power Company，Zhengzhou Henan 450052，China)

Abstract：With the advancement of the "Dual Carbon" strategy, the distribution network is transitioning from a traditional unidirectional radial supply to an active distribution network with the participation of multiple distributed power sources. The distribution cloud master station, which collects data from various distributed power sources and achieves multi-source coordination, relies on a sparse communication network and is thus vulnerable to the threat of False Data Injection(FDI) malicious attacks. To counteract the generalized FDI threat with high-frequency and unbounded high-order derivatives, a fully distributed secondary resilient control strategy for active distribution networks is proposed. By leveraging high-order integral suppression coefficients, the FDI in control channels with bounded finite-order derivatives is suppressed. It is proven by the Lyapunov method that the proposed defense strategy can achieve Uniformly Ultimately Bounded(UUB) convergence for frequency regulation and has been verified on an improved IEEE 9-bus active distribution network.

Keywords：active distribution networks；distributed control；resilient control；False Data Injection；distribution cloud master station

随着“双碳”战略的持续推进，光伏、储能、电动汽车等分布式电源广泛接入，配电网由传统单向辐射供给向多环节协同的有源配电网转变[1]。考虑到多区域有源配电网内源、荷、储等各主体接入下的实时调控需求，构建配电云主站实现有源配电网信息化转型成为提升有源配电网自治能力[2]、实现分布式新能源最大化就地消纳、兼顾配电网协同实现区域电力电量平衡的关键[3]。因此，融合了配电网物理设备与分布式控制器及协同通信

收稿日期：2024-11-12；**修回日期：**2024-12-29

基金项目：国家电网河南省电力公司科技资助项目(52170223000T)

引用格式：刘昊,张凯,郭祥富,等. 考虑广义FDI攻击的配电云主站韧性协同控制[J]. 太赫兹科学与电子信息学报, 2025,23(7):685-691. DOI:10.11805/TKYDA2024591.

Citation format：LIU Hao,ZHANG Kai,GUO Xiangfu,et al. Resilient coordinated control of distribution cloud master station considering generalized FDI attacks[J]. Journal of Terahertz Science and Electronic Information Technology, 2025,23(7):685-691. DOI:10.11805/TKYDA2024591.

网络的有源配电网成为典型的信息物理系统[4]。配电云主站作为信息集成平台，需处理和协调来自分布式电源的大量数据，同时需确保数据的安全性和可靠性，以抵御潜在的网络攻击。

分布式二次控制因其灵活性、可扩展性和鲁棒性被视为一种实现有源配电网自治与互济协同的可行策略[5]。但基于分布式二次控制的协同策略依赖于稀疏通信网络获取邻居节点状态信息[6]，稀疏通信网络下分布式协同的远程可控性及用户侧信息安全防护措施的脆弱性使末端有源配电网分布式协同面临信息安全风险。具体而言，末端配电网源、荷、储等要素与用户频繁互动，互动环节存在大量影响信息调控的开放接口，攻击者以错误数据注入的形式通过开放接口的薄弱环节进行攻击[7]。攻击包含多个频率、维度及时间尺度下的耦合注入，在时域特征上表现出对时间的多阶次导数无界。这种广义外部故障注入型攻击(FDI)成为一种威胁能源系统安全的新型攻击手段，破坏低压有源配电网的整体性能和稳定性[8]。现有的抗FDI协同研究主要集中在两类应对网络物理攻击的方法上：一类方法是检测受损代理，然后采取恢复或隔离策略[9]。但存在隐蔽的FDI攻击可以绕过现有的电力系统攻击检测算法，潜在多重复杂耦合攻击者发起的FDI隐形攻击无法检测[10]。因此，通过设计抗攻击协同控制策略，增强海量分布电源接入下的有源配电网台区自治韧性与自我恢复能力，成为保护新型电力系统末端配用电安全的关键任务[11]。具体来说，需设计一类分布式抗攻击韧性控制策略，缓解一般工况下外部扰动及系统内部广义FDI的不利影响[12]。考虑到海量分布式电源接入，应针对单个分布式电源节点设计本地分布式控制方法[13]，无需检测和识别被破坏的分布式节点[14]，同时增强有源配电网抵御恶意攻击的自我恢复能力[15]。

值得注意的是，在现有文献中，干扰、噪音、故障或攻击一般都被视为有界信号，或一阶时间导数必须是有界的。但攻击者可能会故意向网络物理系统发射无界注入信号，以最大限度地造成破坏。因此，开发能够抵御广义FDI的信息物理协同分布式二次韧性控制策略，对于确保有源配电网的可靠性和安全性至关重要。本文针对有源配电网台区自治的二次频率和电压控制，提出了全分布式抗攻击韧性策略。所提出的抗攻击韧性策略可处理更普遍的无界攻击信号，对有界高阶时间导数的限制更为宽松，增强了有源配电网对恶意网络物理攻击的防御能力。基于Lyapunov稳定性分析表明，针对控制输入通道上的广义FDI攻击，所提出的分布式韧性控制策略在频率调节、电压控制和功率共享方面实现了均匀最终有界(UUB)收敛。

1 问题描述

1.1 通信拓扑

通信网络采用一个时不变加权有向图$\boldsymbol{G}$表示，包含N个分布式电源接入节点，领导节点用于表示有源配电网与大电网衔接节点。定义$d_i=\sum_{j=1}^{n}a_{ij}$，d_i为i节点的衔接集总，a_{ij}用于表征i节点与j节点的联通状态。该有向图对应的邻接矩阵为$\boldsymbol{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$，$\boldsymbol{D}=\mathrm{diag}(d_i)\in\mathbb{R}^{N\times N}$、$\boldsymbol{L}=\boldsymbol{D}-\boldsymbol{A}$分别为入度矩阵和相应的拉普拉斯矩阵。定义领导节点$k$用于提供上限和下限参考值；$g_{ik}$为从第$k$个领导节点到第$i$个逆变器的固定增益，汇总在对角矩阵$\boldsymbol{G}_k=\mathrm{diag}(g_{ik})$中；$\sigma_{\min}(\cdot)$和$\sigma_{\max}(\cdot)$分别为给定矩阵的最小和最大奇异值。

1.2 攻击描述

考虑交流有源配电网的二次频率和电压控制的抗攻击防御问题。攻击注入预设如图1所示，对于第i个分布式单元，基准下垂控制描述为：

$$\omega_i=\omega_{ni}-m_{Pi}P_i \tag{1}$$

$$v_{odi}=V_{ni}-n_{Qi}Q_i \tag{2}$$

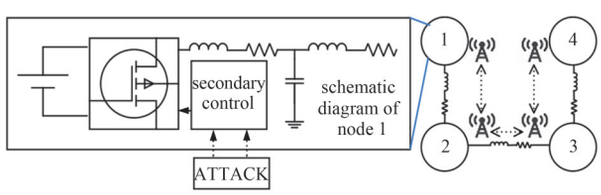


Fig.1 Schematic diagram of question pre-setting

图1 问题预设示意图

式中：P_i和Q_i分别为有功功率和无功功率；ω_i和v_{odi}分别为端电压的运行角频率和三相坐标系到旋转坐标系dq0变换(帕克变换)的d分量；ω_{ni}和V_{ni}是从二次控制层馈送的初级下垂机制的设定值；m_{Pi}和n_{Qi}是根据逆变器的功率等级选择的$P-\omega$和$Q-v$下垂系数。

对式(1)~(2)的下垂关系进行时间求导，得

$$\dot{\omega}_{ni}=\dot{\omega}_i+m_{Pi}\dot{P}_i=u_{fi} \tag{3}$$

$$\dot{V}_{ni}=\dot{v}_{odi}+n_{Qi}\dot{Q}_i=u_{vi} \tag{4}$$

式中u_{fi}和u_{vi}为待设计的控制输入。

进一步考虑交流有源配电网的二次频率和电压控制的抗攻击防御问题。实际系统中，由用户交互渠道注入的FDI攻击以系统宕机为目的，表现为振幅持续增加的振荡形式，在数据特征上表现为攻击信号一阶导数无界但高阶导数有界[25]。此类FDI注入往往引入了对频率和电压控制回路局部输入通道的一般性无界FDI攻击：

$$\dot{\omega}_{ni}=u_{fi}+\Delta_{fi} \tag{5}$$

$$\dot{V}_{ni}=u_{vi}+\Delta_{vi} \tag{6}$$

式中 Δ_{fi} 和 Δ_{vi} 分别表示注入到第 i 个逆变器的频率和电压控制回路输入通道中的无界攻击信号。$\Delta_{fi}(t)\in C^{\gamma}$ 且 $\Delta_{vi}(t)\in C^{\gamma}$，$C^{\gamma}$ 表示变量本身及其 γ 阶导数有界，则有：

$$\left|\frac{d^{\gamma}}{\mathrm{d}t^{\gamma}}\Delta_{vi}\right|\leqslant\kappa_{vi} \tag{7}$$

$$\left|\frac{d^{\gamma}}{\mathrm{d}t^{\gamma}}\Delta_{fi}\right|\leqslant\kappa_{fi} \tag{8}$$

式中 κ_{fi} 和 κ_{vi} 为常数。

1.3 控制目标

由于 Δ_{fi} 和 Δ_{vi} 是无界的，传统的协同控制协议无法在接受范围内调节频率和控制电压。因此，需要抗攻击防御策略保持频率调节和电压控制性能，并确保闭环稳定性。控制目标可表述为：

信号 $x(t)$ 是一致最终有界(UUB)的，其最终界为 b，如果存在正数 b 和 c，以及对于每一个 $a\in(0,c)$，存在一个非负数 $t_1=t_1(a,b)\geqslant 0$，使得对于任意的 $t\geqslant t_0$，当 $\|x(t_0)\|\leqslant a$ 时，对于所有 $t\geqslant t_0+t_1$，都有 $\|x(t)\|\leqslant b$。

抗攻击频率防御：设计每个逆变器的输入控制信号 u_{fi}，使得在局部频率控制回路遭受一般性无界攻击的情况下，全局频率控制误差 e_f 保持UUB。

抗攻击电压防御：设计每个逆变器的输入控制信号 u_{vi}，使得在局部电压控制回路遭受一般性无界攻击的情况下，全局电压控制误差 e_v 保持UUB。

2　有源配电网全分布式韧性控制

2.1 主导跟随式全分布式二次控制

考虑到有源配电网自治台区需配合上级配电网及配电网子站、主站统一调控需求，协同实现区域电力电量平衡的任务需求，选择配电网与主电网通过变压器节点衔接，该节点可视为有源配电网体系中存在“主导节点”。为将每个逆变器的端口频率调节到参考值，并将每个逆变器的端子电压保持在可接受范围内，设计了基于主导–跟随者的二次控制。使用与相邻逆变器和领导者相关的相对信息，本地的协同频率和电压控制协议为：

$$u_{f_i}=c_{f_i}\sum_{j\in F}a_{ij}\left(\omega_j-\omega_i\right)+c_{f_i}\sum_{k\in L}g_{ik}\left(\omega_k-\omega_i\right)+c_{f_i}\sum_{j\in F}a_{ij}\left(m_{P_j}P_j-m_{P_i}P_i\right) \tag{9}$$

$$u_{v_i}=c_{v_i}\sum_{j\in F}a_{ij}\left(v_{odj}-v_{odi}\right)+c_{v_i}\sum_{k\in L}g_{ik}\left(v_k-v_{odi}\right)+c_{v_i}\sum_{j\in F}a_{ij}\left(n_{Q_j}Q_j-n_{Q_i}Q_i\right) \tag{10}$$

式中：c_{fi} 和 c_{vi} 为增益常数；$F=\{1,2,\cdots,N\}$；$L=\{N+1,N+2\}$。一次控制层的设定点 ω_{ni} 和 V_{ni} 随后从 u_{fi} 和 u_{vi} 计算得出：

$$V_{ni}=\int u_{vi}\mathrm{d}t \tag{11}$$

$$\omega_{ni}=\int u_{fi}\mathrm{d}t \tag{12}$$

利用式(9)~(10)将式(3)~(4)重写为：

$$\dot{\omega}_{n_i}=c_{f_i}\left(\sum_{j\in F}a_{ij}\left(\omega_{n_j}-\omega_{n_i}\right)+\sum_{k\in L}g_{ik}\left(\omega_{n_k}-\omega_{n_i}\right)\right) \tag{13}$$

$$\dot{V}_{n_i}=c_{v_i}\left(\sum_{j\in F}a_{ij}\left(V_{n_j}-V_{n_i}\right)+\sum_{k\in L}g_{ik}\left(V_{n_k}-V_{n_i}\right)\right) \tag{14}$$

式中：$\omega_{nk}=\omega_k+m_{P_i}P_i$；$V_{nk}=v_k+n_{Q_i}Q_i$。

定义 $\boldsymbol{\Phi}_k=0.5L+G_k$，则式(9)~(10)的全局形式为：

$$\dot{\boldsymbol{\omega}}_n=-\mathrm{diag}\left(c_{f_i}\right)\sum_{k\in\mathcal{L}}\boldsymbol{\Phi}_k\left(\boldsymbol{\omega}_n-\mathbf{1}_N\otimes\omega_{n_k}\right) \tag{15}$$

$$\dot{\boldsymbol{V}}_n=-\mathrm{diag}\left(c_{v_i}\right)\sum_{k\in\mathcal{L}}\boldsymbol{\Phi}_k\left(\boldsymbol{V}_n-\mathbf{1}_N\otimes V_{n_k}\right) \tag{16}$$

式中：$\boldsymbol{\omega}_n=\left[\omega_{n1}^{\mathrm{T}},\omega_{n2}^{\mathrm{T}},\cdots,\omega_{nN}^{\mathrm{T}}\right]^{\mathrm{T}}$；$\boldsymbol{V}_n=\left[V_{n1}^{\mathrm{T}},V_{n2}^{\mathrm{T}},\cdots,V_{nN}^{\mathrm{T}}\right]^{\mathrm{T}}$；$\mathbf{1}_N\in\mathbb{R}^N$为一个所有元素均为1的列向量。将包含全局频率和电压的误差向量定义为：

$$\boldsymbol{e}_f=\boldsymbol{\omega}_n-\left(\sum_{k\in L}\boldsymbol{\Phi}_k\right)^{-1}\sum_{k\in L}\boldsymbol{\Phi}_k\left(\mathbf{1}_N\otimes\omega_{n_k}\right) \tag{17}$$

$$\boldsymbol{e}_v=\boldsymbol{V}_n-\left(\sum_{k\in L}\boldsymbol{\Phi}_k\right)^{-1}\sum_{k\in L}\boldsymbol{\Phi}_k\left(\mathbf{1}_N\otimes V_{n_k}\right) \tag{18}$$

当从每个主导节点到每个逆变器存在一个有向路径时，$\sum_{k\in L}\boldsymbol{\Phi}_k$是非奇异且正定的。如果$\lim_{t\to\infty}\boldsymbol{e}_f(t)=0$、$\lim_{t\to\infty}\boldsymbol{e}_v(t)=0$，则频率和电压控制目标实现。考虑到无界攻击$\Delta_{fi}$和$\Delta_{vi}$下稳定性难以保证，因此考虑设定补偿项，实现应对无界FDI的全分布式韧性二次控制。

2.2 全分布式抗攻击韧性二次控制

为应对无界攻击Δ_{fi}和Δ_{vi}，提出完全分布式抗攻击防御策略，解决抗攻击频率和电压防御问题，定义：

$$\theta_{fi}=c_{fi}\left(\sum_{j\in F}a_{ij}\left(\omega_{nj}-\omega_{ni}\right)+\sum_{k\in L}g_{ik}\left(\omega_{nk}-\omega_{ni}\right)\right) \tag{19}$$

$$\theta_{vi}=c_{vi}\left(\sum_{j\in F}a_{ij}\left(V_{nj}-V_{ni}\right)+\sum_{k\in L}g_{ik}\left(V_{nk}-V_{ni}\right)\right) \tag{20}$$

然后，针对频率和电压控制回路提出了以下抗攻击防御策略：

$$ur_{fi}=\theta_{fi}\left(\frac{1+\chi_{fi}}{\left|\theta_{vi}\right|+\eta_{fi}}\right),\ \chi_{fi}^{(\alpha)}=\beta_{fi}\left|\theta_{fi}\right| \tag{21}$$

$$ur_{vi}=\theta_{vi}\left(\frac{1+\chi_{vi}}{\left|\theta_{vi}\right|+\eta_{vi}}\right),\ \chi_{vi}^{(\alpha)}=\beta_{vi}\left|\theta_{vi}\right| \tag{22}$$

式中：η_{fi}和η_{vi}为正的指数衰减函数；χ_{fi}和χ_{vi}为自适应调谐参数，χ_{fi}和χ_{vi}的初值为正；适应增益β_{fi}和β_{vi}为给定的常数。

图2为提出的二次控制策略。对设定的无界FDI，实施如式(19)所述的协同抗攻击电压防御策略时，定义的误差$\boldsymbol{e}_f$是UUB的，即解决了抗攻击频率防御问题。此外，通过适当调整式(21)中β_{fi}的值，$\boldsymbol{e}_f$的最终界限可被缩小到任意小。

证明：结合式(13)、式(15)和式(19)得到全局形式：

$$\dot{\boldsymbol{\theta}}_f=-\left(\sum_{k\in L}\boldsymbol{\Phi}_k\right)\mathrm{diag}\left(c_{fi}\right)\dot{\boldsymbol{\omega}}_n=-\left(\sum_{k\in L}\boldsymbol{\Phi}_k\right)\mathrm{diag}\left(c_{fi}\right)\left(\frac{\boldsymbol{\theta}_f+\boldsymbol{\Delta}_f+\theta_{fi}\chi_{fi}}{\left|\theta_{fi}\right|+\eta_{fi}}\right) \tag{23}$$

式中：$\boldsymbol{\theta}_f=\left[\theta_{f1}^{\mathrm{T}},\theta_{f2}^{\mathrm{T}},\cdots,\theta_{fN}^{\mathrm{T}}\right]^{\mathrm{T}}$；$\boldsymbol{\Delta}_f=\left[\Delta_{f1}^{\mathrm{T}},{}_{f2}^{\mathrm{T}},\cdots,\Delta_{fN}^{\mathrm{T}}\right]^{\mathrm{T}}$。

考虑以下Lyapunov函数：

$$V=0.5\boldsymbol{\theta}_f^{\mathrm{T}}\left(\sum_{k\in L}\boldsymbol{\Phi}_k\right)^{-1}\boldsymbol{\theta}_f \tag{24}$$

对时间求导有以下条件成立：

$$\dot{V}\leqslant-\sigma_{\min}\operatorname{diag}\left(c_{f_i}\right)\left\|\boldsymbol{\theta}_f\right\|^2-\operatorname{diag}\left(c_{f_i}\right)\sum_{i\in F}\left(\theta_{f_i}\times\frac{\theta_{fi}\chi_{fi}}{\left|\theta_{fi}\right|+\eta_{fi}}\right)+\operatorname{diag}\left(c_{f_i}\right)\sum_{i\in F}\left|\theta_{f_i}\right|\left|\Delta_{f_i}\right| \tag{25}$$

式中：$\operatorname{diag}\left(c_{f_i}\right)\sum_{i\in F}\left|\theta_{f_i}\right|\left|\Delta_{f_i}\right|-\operatorname{diag}\left(c_{f_i}\right)\sum_{i\in F}\left(\theta_{f_i}(\theta_{fi}\chi_{fi}/(\left|\theta_{fi}\right|+\eta_{fi}))\right)=\operatorname{diag}\left(c_{f_i}\right)\sum_{i\in F}\left(\left|\theta_{f_i}\right|\dfrac{\left(\left|\theta_{f_i}\right|\left(\left|\Delta_{f_i}\right|-\chi_{f_i}\right)+\left|\Delta_{f_i}\right|\eta_{f_i}\right)}{\left|\theta_{f_i}\right|+\eta_{f_i}}\right)$

结合1.2节攻击描述中FDI的定义，有$\exists t_2>t_1$使得$\forall t\geqslant t_2$，下列条件成立：

$$\operatorname{diag}\left(c_{f_1}\right)\sum_{i\in F}\left|\zeta_{f_1}\right|\left|\Delta_{f_1}\right|\leqslant\operatorname{diag}\left(c_{f_1}\right)\sum_{i\in F}\left(\zeta_{f_1}\Lambda_{f_1}\right) \tag{26}$$

综上，有下列条件成立：

$$\dot{V}\leqslant 0,\forall\left|\boldsymbol{\theta}_f\right|\geqslant\kappa_f/\beta_f,\forall t\geqslant t_2 \tag{27}$$

因此，$\boldsymbol{\theta}_f$是UUB的。在系统保持稳定的情况下，适应增益β_f的值越大，最终边界就越小；又有$\boldsymbol{\theta}_f=\sum_{k\in\mathcal{L}}\boldsymbol{\Phi}_k\boldsymbol{e}_f$。因此，$\boldsymbol{e}_f$也是有界的。同理可得，电压偏差$\boldsymbol{e}_v$为UUB，即抗攻击电压防御问题得以解决。

证毕。

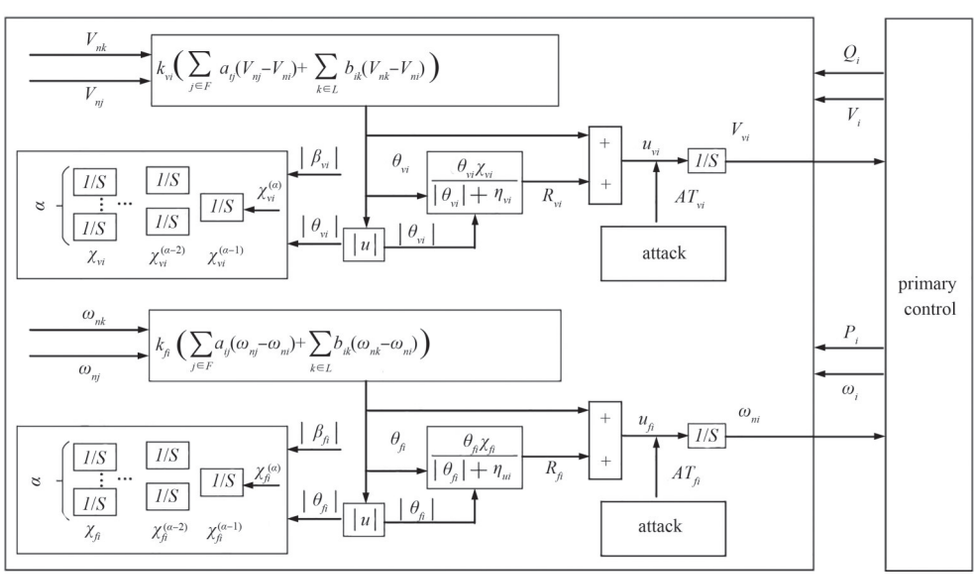


Fig.2 Block diagram of proposed secondary control

图2 所提二次控制框图

3　仿真验证

如图3所示，在一个改进的IEEE 9节点系统验证所提出的全分布式抗攻击二级防御策略。IEEE 9节点系统在总线100处被孤岛化，包含3个基于逆变器的分布式电源节点(Distributed Energy Resources，DERs)和领导者。所有逆变器的额定功率相同，逆变器下垂增益设定为$m_{P1}=9.4\times10^{-5}$，$m_{P2}=18.8\times10^{-5}$，$m_{P3}=28.2\times10^{-5}$，$n_{Q1}=1.3\times10^{-3}$，$n_{Q2}=2.6\times10^{-3}$，$n_{Q3}=3.9\times10^{-3}$。逆变器在双向通信网络上通信，邻接矩阵$\boldsymbol{A}=[0\,1\,1;1\,0\,1;1\,1\,0]$。河南某地23节点示范工程下垂增益设定为$m_P=1\times10^{-5}$，$n_Q=1\times10^{-3}$，邻接矩阵$\boldsymbol{A}=[0\,1\,0\,1;1\,0\,1\,0;0\,1\,0\,1;1\,0\,1\,0]$。两系统增益$g=1$。频率基准、电压上限基准和电压下限基准分别为50 Hz、390 V

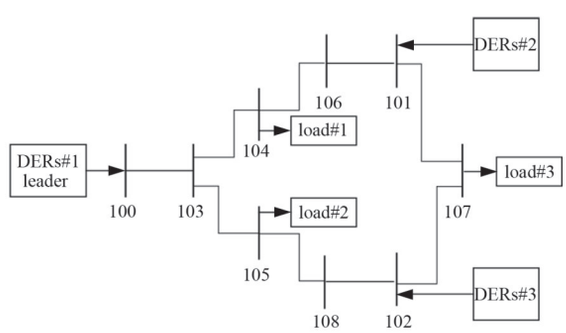
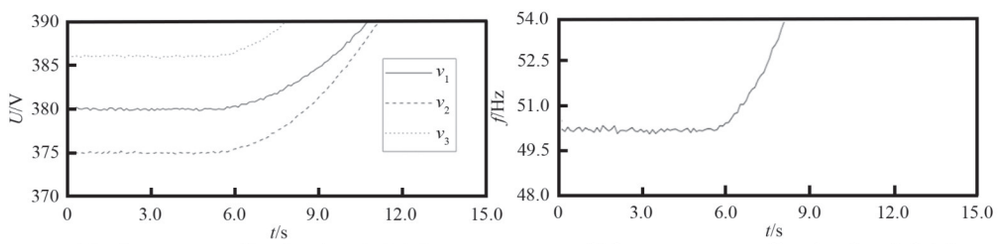


Fig.3 Improved IEEE 9 node and equivalent schematic diagram

图3 改进IEEE 9节点及等效示意图

和370 V。

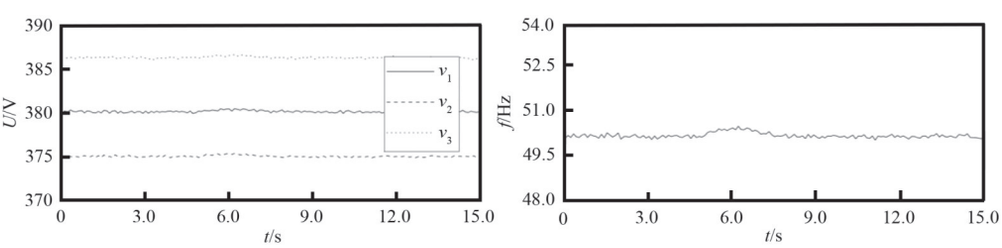
在IEEE 9节点系统中，频率和电压控制回路的无约束攻击注入分别设为：$AT_{v1}=0.5t^2$、$AT_{v2}=0.4t^2$、$AT_{v3}=0.3t^2$、$AT_{f1}=0.3t^2$、$AT_{f2}=0.4t^2$、$AT_{f3}=0.5t^2$。将抗攻击防御策略的性能与式(9)~(10)中的传统二次控制方法进行比较。控制协议的恒定频率增益设为20，恒定电压增益设为10；抗攻击防御策略的适应增益设为$\beta_{vi}=20(i=1,2,3)$，$\beta_{fi}=350$。图4~5为使用传统基准策略和本文所提策略应对无限制攻击时的电压和频率响应结果。从图5可以看出，t=5 s开始注入攻击后，传统方法无法保持系统稳定性，电压和频率都出现了发散。相比之下，所提出的抗攻击二次防御策略，每个逆变器的电压收敛至370~390 V范围内，频率收敛至参考值50 Hz。上述结果验证了所提出的弹性防御策略能够在频率调节方面实现收敛。图6为逆变器频率与时间关系图，通过适当调整β_{fi}值，极限约束得以降低，瞬态响应得到改善。



(a) voltage response of benchmark control strategy (b) frequency response of benchmark control strategy

Fig.4 Frequency and d-axis voltage of conventional strategy under generalized FDI attacks

图4 广义FDI攻击下传统策略频率及电压响应



(a) voltage response of proposed strategy (b) frequency response of proposed strategy

Fig.5 Frequency and d-axis voltage of the proposed strategy under generalized FDI attacks

图5 广义FDI攻击下所提策略频率及电压响应

4 结论

本文提出了针对有源配电网的新型二次网络物理防御策略，以抵御对频率和电压控制回路输入通道的一般无限制攻击。所提出的全分布式网络物理防御策略基于自适应控制技术，通过保持频率调节的UUB共识和实现电压抑制，确保闭环系统的UUB稳定性。此外，还可通过适当调整自适应增益调整收敛的最终边界。利用改进的IEEE 9系统验证了所提出的抗广义FDI攻击韧性。

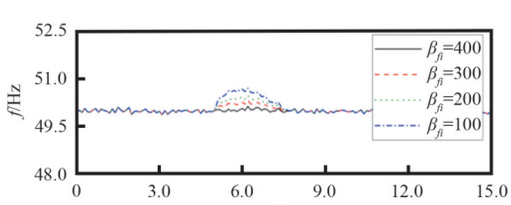


Fig.6 Comparison of frequency performance under generalized FDI attacks at different time

图6 广义FDI攻击下的频率性能比较

参考文献：

[1] 韩肖清,李廷钧,张东霞,等. 双碳目标下的新型电力系统规划新问题及关键技术[J]. 高电压技术, 2021,47(9):3036-3046. (HAN Xiaoqing,LI Tingjun,ZHANG Dongxia,et al. New issues and key technologies of new power system planning under double carbon goals[J]. High Voltage Engineering, 2021,47(9):3036-3046.)

[2] 张国驹,裴玮,杨鹏,等. 中压配电网柔性互联设备的电路拓扑与控制技术综述[J]. 电力系统自动化, 2023,47(6):18-29. (ZHANG Guoju, PEI Wei, YANG Peng, et al. Review on circuit topology and control technology of flexible interconnection devices for medium-voltage distribution network[J]. Automation of Electric Power Systems, 2023,47(6):18-29.) DOI:10.7500/AEPS20221030004.

[3] 杨挺,刘亚闯,刘宇哲,等. 信息物理系统技术现状分析与趋势综述[J]. 电子与信息学报, 2021,43(12):3393-3406. (YANG Ting,LIU Yachuang,LIU Yuzhe,et al. Review on cyber-physical system:technology analysis and trends[J]. Journal of Electronics

& Information Technology, 2021,43(12):3393-3406.) DOI:10.11999/JEIT211135.

[4] 张洪略,万毅,王家军,等. 基于数据挖掘算法的电网调度信号异常数据提取方法[J]. 太赫兹科学与电子信息学报, 2024, 22(7):800-806. (ZHANG Honglve,WAN Yi,WANG Jiajun, et al. Abnormal data extracting from power grid dispatching signals based on data mining algorithms[J]. Journal of Terahertz Science and Electronic Information Technology, 2024,22(7):800-806.) DOI:10.11805/TKYDA2023381.

[5] 杨向真,苏建徽,丁明,等. 面向多逆变器的微电网电压控制策略[J]. 中国电机工程学报, 2012,32(7):7-13. (YANG Xiangzhen, SU Jianhui,DING Ming, et al. Voltage control strategies for microgrid with multiple inverters[J]. Proceedings of the CSEE, 2012, 32(7):7-13.)

[6] 刘畅,卓建坤,赵东明,等. 利用储能系统实现可再生能源微电网灵活安全运行的研究综述[J]. 中国电机工程学报, 2020, 40(1):1-18. (LIU Chang,ZHUO Jiankun,ZHAO Dongming,et al. A review on the utilization of energy storage system for the flexible and safe operation of renewable energy microgrids[J]. Proceedings of the CSEE, 2020,40(1):1-18.) DOI:10.13334/j.0258-8013.pcsee.190212.

[7] TADEPALLI P S,PULLAGURAM D. Distributed control microgrids: cyber-attack models, impacts and remedial strategies[J]. IEEE Transactions on Signal and Information Processing Over Networks, 2022(8): 1008-1023. DOI: 10.1109/TSIPN. 2022. 3230562.

[8] ZHANG J Q,SAHOO S,PENG J C H,et al. Mitigating concurrent false data injection attacks in cooperative DC microgrids[J]. IEEE Transactions on Power Electronics, 2021,36(8):9637-9647. DOI:10.1109/TPEL.2021.3055215.

[9] MO Y L,SINOPOLI B. On the performance degradation of cyber-physical systems under stealthy integrity attacks[J]. IEEE Transactions on Automatic Control, 2016,61(9):2618-2624. DOI:10.1109/TAC.2015.2498708.

[10] XIAO Xuanyi, ZHOU Quan, WANG Feng, et al. Three-stage defensive framework for distributed microgrid control against cyberattacks[J]. Journal of Modern Power Systems and Clean Energy, 2022,10(6):1669-1678. DOI:10.35833/MPCE.2021.000333.

[11] CHEN Yulin, QI Donglian, DONG Hangning, et al. A FDI attack-resilient distributed secondary control strategy for islanded microgrids[J]. IEEE Transactions on Smart Grid, 2021,12(3):1929-1938. DOI:10.1109/TSG.2020.3047949.

[12] VEERASAMY V,HU Z J,QIU H F,et al. Blockchain-enabled peer-to-peer energy trading and resilient control of microgrids[J]. Applied Energy, 2024(353):122107. DOI:10.1016/j.apenergy.2023.122107.

[13] HUANG T,WU D,ILIĆ M. Cyber-resilient automatic generation control for systems of AC microgrids[J]. IEEE Transactions on Smart Grid, 2024,15(1):886-898. DOI:10.1109/TSG.2023.3272632.

[14] DENG Chao, WANG Yu, WEN Changyun, et al. Distributed resilient control for energy storage systems in cyber-physical microgrids[J]. IEEE Transactions on Industrial Informatics, 2021,17(2):1331-1341. DOI:10.1109/TII.2020.2981549.

[15] SHI Mengxuan, CHEN Xia, SHAHIDEHPOUR M, et al. Observer-based resilient integrated distributed control against cyberattacks on sensors and actuators in islanded AC microgrids[J]. IEEE Transactions on Smart Grid, 2021,12(3):1953-1963. DOI:10.1109/TSG.2021.3050203.

作者简介：

刘　昊(1977-)，男，博士，高级工程师，主要研究方向为微电网控制.email:liuhaoepri@139.com.

张　凯(1974-)，男，硕士，教授级高级工程师，主要研究方向为配电网标准化设计及概预算自动统计.

郭祥富(1983-)，男，硕士，教授级高级工程师，主要研究方向为配电物联网、电力信息化.

胡誉蓉(1997-)，女，硕士，助理工程师，主要研究方向为谐波分析与治理.

贺　翔(1973-)，男，学士，高级工程师，主要研究方向为智能配电网.

赵　健(1988-)，男，博士，高级工程师，主要研究方向为电力系统及其自动化.