# FDI 攻击下孤岛交流微电网滑模控制策略*

王 君[1],冯 甜[2]
(1.甘肃省全国工业生产过程先进质量控制系统重点技术实验室,甘肃 兰州 730050;
2.兰州理工大学 电气工程与信息工程学院,甘肃 兰州 730050)

**摘 要**:针对孤岛交流微电网控制系统中不可避免的虚假数据注入攻击问题,当存在外部干扰时,设计了主动容侵控制策略。首先针对孤岛交流微电网逆变系统,构建系统状态空间模型。将控制系统传感器侧可能受到的虚假数据注入攻击信息当作一个辅助状态向量,设计滑模攻击观测器对系统中的状态变量和虚假数据注入攻击信息同时进行估计。在获得攻击的估计信息后,利用积分滑模容侵控制器对虚假数据注入攻击和外部有限能量干扰进行主动容侵控制,以确保微电网系统的稳定运行。最后,通过仿真验证了所提方法的可行性和有效性。

**关键词**:微电网;虚假数据注入攻击;滑模观测器;容侵控制
**中图分类号**:TP391 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.212359

**中文引用格式**:王君,冯甜. FDI 攻击下孤岛交流微电网滑模控制策略[J].电子技术应用,2022,48(12):89-93,99.
**英文引用格式**:Wang Jun,Feng Tian. Sliding-mode control strategy of island AC microgrid under FDI attack[J]. Application of Electronic Technique,2022,48(12):89-93,99.

# Sliding-mode control strategy of island AC microgrid under FDI attack

Wang Jun[1],Feng Tian[2]
(1.Key Lab of Advanced Control for Industrial Process in Gansu Province,Lanzhou 730050,China;
2.College of Electrical and Information Engineering,Lanzhou University of Technology,Lanzhou 730050,China)

**Abstract**: In this paper, an active intrusion tolerance control strategy is designed for the inevitable false data injection attack in the control system of island AC microgrid when there is external interference. Firstly, the state space model of the island AC microgrid inverter system is constructed. A sliding-mode attack observer is designed to estimate both the state variables and the false data injection attack information in the control system. After obtaining the estimated information of the attack, the integrated sliding mode intrusion tolerance controller is used to actively control the false data injection attack and external finite energy interference to ensure the stable operation of the microgrid system. Finally, the feasibility and effectiveness of the proposed method are verified by simulation.

**Key words**: microgrid; FDI attack; sliding-mode observer; intrusion tolerant control

## 0 引言

电力信息物理系统是智能电网与信息物理系统的有机结合,先进的信息技术给电力系统控制带来便利的同时也伴随着潜在负面影响。大量的研究指出,信息网中原有的各类安全风险(如网络攻击)极易被引入到电力网中而使得系统变得脆弱[1]。数据注入攻击是一种典型的网络攻击方式,通过破坏电力信息物理系统的数据完整性来干扰决策,成功躲避坏数据检测机制,达到危及电力信息物理系统安全的目的。

微电网是电力信息物理系统的一种且虚假数据注入攻击也是微电网中最常见的攻击。对微电网信息物理系统实施虚假数据注入攻击主要指:攻击者利用设备漏洞,在信息采集、传输或计算环节蓄意注入错误数据,通过破坏数据的真实性使控制目标发生偏离,进而达到破坏系统稳定性的目的。常值虚假数据注入攻击指攻击信号为常值的虚假数据注入攻击。可见,常值虚假数据注入攻击是最简单的一种虚假数据注入攻击形式。虚假数据注入攻击在分布式控制中具有一定的隐蔽性。原因之一在于攻击者不会采用幅值过大的注入数据,使系统产生发生正常扰动的错觉,否则将会引起系统的警觉。对微电网分布式控制而言,常值虚假数据注入攻击具有一定的隐蔽性和破坏性[2]。因此,虚假数据注入攻击的检测与重构对微电网的安全与稳定运行具有重要意义。

作为针对基础工业控制系统的一种新型攻击方式,虚假数据注入攻击的攻击原理、检测算法等都亟待进一步研究[3-4]。对于遭受网络攻击的电力信息物理系统,直

*基金项目:国家自然科学基金(61463030)

觉上可以将网络攻击与传感器故障、执行器故障等进行类比，已有的故障检测方法可以启迪攻击问题的研究。现有的研究大多只考虑了网络攻击的检测问题，如文献[5]提出了基于卡尔曼滤波的电力虚假数据注入攻击的检测方法；文献[6]针对一类非线性系统的虚假数据注入攻击进行估计；文献[7]采用一种基于时序近邻保持嵌入的方法来检测智能电网中是否存在虚假数据注入攻击；文献[8]提出一种基于聚类算法与状态预测检测法的虚假数据注入攻击检测技术；文献[9]针对微电网环境下虚假数据注入攻击的状态估计问题，提出了一种基于分析状态测量值增量的攻击检测机制。而上述文献对虚假数据注入攻击的防御问题未做研究，为了防御攻击以保护系统，相关学者根据其造成的影响制定了相应对策。文献[10]针对虚假数据注入攻击，为了避免智能电网系统被陌生攻击者发起入侵行为，提出了基于自适应的马尔科夫过程防御策略，来抵抗非显性攻击；文献[11]提出了 Gauss 混合模型的检测方案，可以有效抵抗虚假数据注入攻击；文献[12]中，针对检测已知的网络攻击模型以对抗攻击，作者基于区间状态估计的设计理念，提出了一种全新的网络攻击抵抗机制。以上文献主要针对电力信息物理系统受到虚假数据注入攻击时的检测与防御问题，当电力信息物理系统尤其是微电网系统同时又受到负载小扰动或分布式电源功率波动等干扰时，系统的安全运行问题会变得更加复杂，而此类研究还很少涉足。

综上所述，本文针对孤岛模式下微电网逆变系统的拓扑结构，考虑到可能存在的外部干扰，建立受到虚假数据注入攻击的增广状态空间描述；受已有观测器设计方法启发[13]，设计相应的滑模攻击估计观测器对网络攻击信息进行实时估计。当获得准确的攻击信息时，为提高系统的鲁棒性，设计积分滑模容侵控制器确保逆变系统在受到虚假数据注入攻击时的稳定性以及抗扰动抑制性。

## 1 问题描述

### 1.1 孤岛逆变系统主电路拓扑

孤岛交流微电网逆变系统主电路拓扑如图 1 所示[14]。逆变器包括直流输入电压源 $U_{dc}$、6 个全控型功率器件 IGBT、开关器件拥有的微小电阻 $R_1$、传输线路中存在的阻抗 $R_2$ 和 LCL 低通滤波器。$U_{dc}$ 表示微电网逆变系统中的直流电源，包括光伏、风电等可再生的能源；系统中各个开关器件上的串联电阻等效为 $R_1$，电能从逆变器输出到达交流母线的过程中也存在电阻，这些低压电阻等效为 $R_2$。LCL 滤波器上与电容串联的电阻为 $R$，流过电感 $L_1$ 的电流为 $i_1$，流过电感 $L_2$ 的电流为 $i_2$。

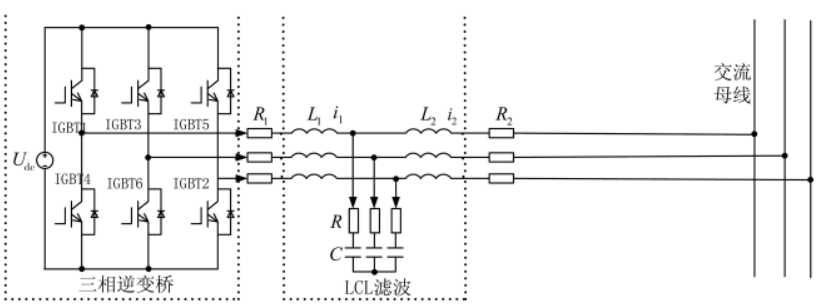



图 1 孤岛交流微电网逆变系统主电路拓扑图

### 1.2 遭受网络攻击的微电网建模

根据孤岛交流微电网逆变系统的结构拓扑，假设系统是理想状态下稳定运行的，将开关损耗和传输线路中的电能损耗考虑在内，采用克拉克变换消除三相中的共模分量，由基尔霍夫电压电流定律可得到孤岛交流微电网 LCL 型逆变器连续的三阶数学模型[15]。

$$\begin{cases} L_1\dfrac{\mathrm{d}i_1}{\mathrm{d}t}=U_o-u_C-R(i_1-i_2)-R_1i_1 \\ L_2\dfrac{\mathrm{d}i_2}{\mathrm{d}t}=u_C+R(i_1-i_2)-R_2i_2 \\ C\dfrac{\mathrm{d}u_C}{\mathrm{d}t}=i_1-i_2 \end{cases} \tag{1}$$

式中，从电感 $L_1$ 上流过的电流为 $i_1$；从电感 $L_2$ 上流过的电流为 $i_2$；经过逆变输出的交流电压为 $U_o$；电容 $C$ 两端的电压为 $u_C$。

定义状态变量 $\boldsymbol{x}(t)=[i_1,i_2,u_C]^{\mathrm{T}}$，关于微电网逆变系统的状态空间表达式如下：

$$\begin{cases} \dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}\boldsymbol{u}(t) \\ \boldsymbol{y}(t)=\boldsymbol{C}\boldsymbol{x}(t) \end{cases} \tag{2}$$

其中：

$$\boldsymbol{A}=\begin{bmatrix} -\dfrac{R+R_1}{L_1} & \dfrac{R}{L_1} & -\dfrac{1}{L_1} \\ \dfrac{R}{L_2} & -\dfrac{R+R_2}{L_2} & \dfrac{1}{L_2} \\ \dfrac{1}{C} & -\dfrac{1}{C} & 0 \end{bmatrix},\boldsymbol{B}=\begin{bmatrix} \dfrac{1}{L_1} \\ 0 \\ 0 \end{bmatrix},\boldsymbol{C}=[1\ \ 1\ \ 0],$$

$\boldsymbol{u}(t)=U_o$。

由于微电网逆变控制系统中可能会受到来自外部的网络攻击如虚假数据注入攻击以及在运行中常常伴有的负载或分布式电源功率波动等扰动，因此系统的状态空间表达式在实际情况下又可表示为：

$$\begin{cases} \dot{\boldsymbol{x}}(t)=\boldsymbol{A}\boldsymbol{x}(t)+\boldsymbol{B}(\boldsymbol{u}(t)+\boldsymbol{w}(t)) \\ \boldsymbol{y}(t)=\boldsymbol{C}\boldsymbol{x}(t)+\boldsymbol{f}_{at}(t) \end{cases} \tag{3}$$

式中，$\boldsymbol{w}(t)$定义为扰动；$\boldsymbol{f}_{at}(t)$表示攻击者构造的攻击向量，当 $i=1$ 时表示测量电流 $i_1$ 的传感器侧受到了虚假数据注入攻击，当 $i=2$ 时表示测量电流 $i_2$ 的传感器侧受到了虚假数据注入攻击，当 $i=3$ 时表示测量电压 $u_C$ 的传感器侧受到了虚假数据注入攻击。线路拓扑中存在较为脆弱的节点，在不同位置上的攻击理论上引发的后果会不同。

## 2 虚假数据注入攻击容侵控制

为消除虚假数据注入攻击对系统稳定性带来的不良后果，针对图 1 所示的孤岛交流微电网系统，设计如图 2 所示的虚假数据注入攻击主动 $H_\infty$ 容侵控制策略结构图。图中滑模攻击估计观测器用于对虚假数据注入攻击信息进行实时估计，积分滑模容侵控制器则会根据实时观测到的系统状态及攻击信息被重新构造以防御攻击实现主动 $H_\infty$ 容侵控制。

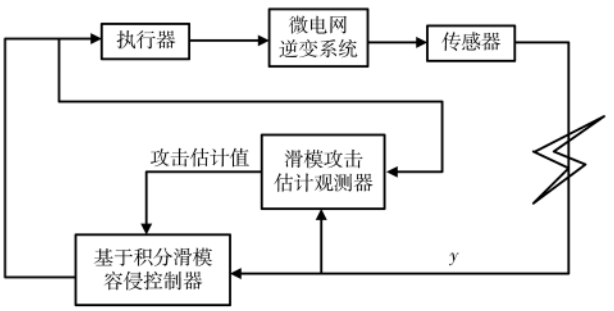



图 2 虚假数据注入攻击容侵控制策略结构图

假设 1 扰动有界，即 $\|w(t)\|\leqslant d$；虚假数据注入攻击有界，即 $\|f_{ai}(t)\|\leqslant\rho$；$d$，$\rho$ 为正数。

### 2.1 滑模攻击估计观测器设计

为了方便得到虚假数据注入攻击与系统状态变量的估计值，将式(3)等价变换为：

$$\begin{cases}\bar{E}\dot{\bar{x}}(t)=\bar{A}\bar{x}(t)+\bar{B}u(t)+\bar{B}_1\bar{F}(t)\\ y(t)=\bar{C}\bar{x}(t)\end{cases}\tag{4}$$

其中，$\bar{x}(t)=\begin{bmatrix}x(t)\\ f_{ai}(t)\end{bmatrix}$，$\bar{A}=\begin{bmatrix}A & 0\\ 0 & -I\end{bmatrix}$，$\bar{B}=\begin{bmatrix}B\\ 0\end{bmatrix}$，$\bar{B}_1=\begin{bmatrix}B & 0\\ 0 & I\end{bmatrix}$，$\bar{F}(t)=\begin{bmatrix}w(t)\\ f_{ai}(t)\end{bmatrix}$，$\bar{C}=[C\quad I]$，$\bar{E}=\begin{bmatrix}I_3 & 0\\ 0 & 0\end{bmatrix}$。

通过等价变换将原系统式(3)中的虚假数据注入攻击 $f_{ai}(t)$ 看作一个状态量，如此可对增广系统式(4)设计有效的状态观测策略，同时估计原始系统状态量和虚假数据注入攻击量。

针对增广系统式(4)，构造滑模状态观测器：

$$\begin{cases}\bar{S}\dot{\bar{r}}(t)=(\bar{A}-\bar{L}_P\bar{C})\hat{\bar{x}}(t)+\bar{L}_Py(t)+\bar{B}u(t)+\bar{L}_Su_S(t)\\ \hat{\bar{x}}(t)=\bar{r}(t)+\bar{S}^{-1}\bar{L}_Dy(t)\end{cases}\tag{5}$$

其中：$\bar{r}(t)$ 为观测器的辅助状态变量，$\hat{\bar{x}}(t)$ 为 $\bar{x}(t)$ 的估计值，$\bar{L}_P$ 和 $\bar{L}_D$ 为待求参数，$u_S(t)$ 是为了消除 FDIA 的影响而引入的不连续滑模输入项，$\bar{L}_S$ 为待求输入项增益。

通过增广系统中的 $\bar{E}$ 和 $\bar{C}$，可以得到如下秩关系：

$$\text{rank}\begin{bmatrix}\bar{E}\\ \bar{C}\end{bmatrix}=\text{rank}\begin{bmatrix}I_3 & 0 & C\\ 0 & 0 & I\end{bmatrix}^{\mathrm{T}}=3+1=4\tag{6}$$

由式(6)可得，一定存在矩阵 $\bar{L}_D\in R^{(3+1)\times1}$ 使得 $\bar{S}=\bar{E}+\bar{L}_D\bar{C}$ 是可逆的。由式(5)可以得到：

$$\bar{S}\dot{\hat{\bar{x}}}(t)=(\bar{A}-\bar{L}_P\bar{C})\hat{\bar{x}}(t)+\bar{B}u(t)+\bar{L}_Py(t)+\bar{L}_Su_S(t)+\bar{L}_D\dot{y}(t)\tag{7}$$

另一方面，在增广系统式(4)的两端同时加上 $\bar{L}_D\dot{y}(t)$，可以得到：

$$\bar{S}\dot{\bar{x}}(t)=(\bar{A}-\bar{L}_P\bar{C})\bar{x}(t)+\bar{B}u(t)+\bar{L}_Py(t)+\bar{L}_D\dot{y}(t)+\bar{B}_1\bar{F}(t)\tag{8}$$

定义误差变量 $\bar{e}(t)=\hat{\bar{x}}(t)-\bar{x}(t)$，根据式(7)和式(8)得到误差动态方程：

$$\dot{\bar{e}}(t)=\bar{S}^{-1}[(\bar{A}-\bar{L}_P\bar{C})\bar{e}(t)+\bar{L}_Su_S(t)-\bar{B}_1\bar{F}(t)]\tag{9}$$

### 2.2 误差系统稳定性分析

设计滑模函数：

$$s_e(t)=\bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P\bar{e}(t)=U\bar{C}\bar{e}(t)\tag{10}$$

其中：$U$ 为待求矩阵，矩阵 $P>0$ 满足 $\bar{B}_1\bar{S}^{-\mathrm{T}}P=U\bar{C}$ 的约束。

构造滑模输入项：

$$u_S(t)=-\phi\text{sgn}(s_e(t))\tag{11}$$

其中，$\phi=v-\rho-d$，$v>0$ 是待求参数。

定理 1 如果非奇异矩阵 $P\in R^{4\times4}>0$，$Y\in R^{4\times4}>0$ 和 $U\in R^{4\times4}>0$ 使得如下约束成立：

$$\begin{cases}P\bar{S}^{-1}\bar{A}-Y\bar{C}+(P\bar{S}^{-1}\bar{A}-Y\bar{C})^{\mathrm{T}}<0\\ \bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P=U\bar{C}\end{cases}\tag{12}$$

则代入滑模输入项 $u_S(t)$ 后误差动态系统是渐进稳定的。进一步，观测器增益 $\bar{L}_P$ 和 $\bar{L}_S$ 可通过下式给出：

$$\bar{L}_P=\bar{S}P^{-1}Y\tag{13}$$

$$\bar{L}_S=\bar{S}P^{-1}\bar{C}^{\mathrm{T}}U^{\mathrm{T}}=\bar{B}_1\tag{14}$$

由于定理 1 中的 $\bar{B}^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P=U\bar{C}$ 不是线性矩阵不等式的形式，无法通过 MATLAB 的 LMI 工具箱进行求解，因此对于 $\varepsilon>0$，建立矩阵不等式：

$$(\bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P-U\bar{C})^{\mathrm{T}}(\bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P-U\bar{C})\leqslant\varepsilon I\tag{15}$$

由 Schur 引理，式(15)等价于：

$$\begin{bmatrix}-\varepsilon I & (\bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P-U\bar{C})^{\mathrm{T}}\\ * & -I\end{bmatrix}\leqslant0\tag{16}$$

由此，定理 1 中的证明问题转换为求满足上述线性矩阵不等式的 $\varepsilon$ 最小值问题。

### 2.3 滑模面可达性分析

以上分析了误差动态系统式(9)稳定的充分条件，本节将分析误差动态系统中滑模面式(10)的可达性问题。

构造 Lyapunov 函数：

$$V_{se}(t)=\frac{1}{2}S_e^{\mathrm{T}}(t)(\bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P\bar{S}^{-1}\bar{B}_1)^{-1}S_e(t)\tag{17}$$

根据误差动态系统式(9)和 $\bar{e}(t)$ 的相应滑模函数(10)，可以得到：

$$S_e(t)=\bar{B}_1^{\mathrm{T}}\bar{S}^{-\mathrm{T}}P\bar{S}^{-1}[(\bar{A}-\bar{L}_P\bar{C})\bar{e}(t)+\bar{L}_Su_S(t)-\bar{B}_1\bar{F}(t)]\tag{18}$$

从而有：

$$\dot{\bar{V}}_{se}(t)=\bar{S}_e^{T}(t)\bar{B}_1^{-1}[(\bar{A}-\bar{L}_P\bar{C})\bar{e}(t)+\bar{L}_S u_S(t)-\bar{B}_1\bar{F}(t)] \tag{19}$$

其中：

$$\bar{S}_e^{T}(t)\bar{B}_1^{-1}[\bar{L}_S u_S(t)-\bar{B}_1\bar{F}(t)]<-\gamma\|S_e(t)\| \tag{20}$$

所以有：

$$\dot{\bar{V}}_{se}(t)<\|S_e(t)\|\{-\gamma+\|(\bar{B}_1^{T}\bar{S}^{-T}P\bar{S}^{-1}\bar{B}_1)^{-1}\times \bar{B}_1^{T}\bar{S}^{-T}P\bar{S}^{-1}(\bar{A}-\bar{L}_P\bar{C})\|\|\bar{e}(t)\|\} \tag{21}$$

定义如下的空间域：

$$\Omega(\delta)=\{-\gamma+\|(\bar{B}_1^{T}\bar{S}^{-T}P\bar{S}^{-1}\bar{B}_1)^{-1}\times \bar{B}_1^{T}\bar{S}^{-T}P\bar{S}^{-1}(\bar{A}-\bar{L}_P\bar{C})\|\|\bar{e}(t)\|<0\} \tag{22}$$

定理 1 中证明了误差动态系统是稳定的，由式(21)可得，$\bar{e}(t)$的轨迹将在有限时间内抵达滑模面 $S_e(t)=0$。

### 2.4 积分滑模容侵控制器设计

当虚假数据注入攻击信息被准确估计后，对估计的攻击信息进行重构，为了提高控制系统的鲁棒性和快速性，设计积分滑模 $H_\infty$ 容侵控制器消除当存在外部干扰时虚假数据注入攻击对系统性能的影响。

将式(7)两边分别减去$\bar{L}_D\bar{C}\dot{\hat{x}}(t)$，可得 $E\dot{\hat{x}}(t)=\bar{A}\hat{x}(t)-\bar{L}_P\bar{C}\bar{e}(t)+\bar{B}u(t)-\bar{L}_D\bar{C}\dot{\bar{e}}(t)+\bar{L}_S u_S(t)$，于是有：

$$\dot{\hat{x}}(t)=A\hat{x}(t)-\bar{L}_{P1}\bar{C}\bar{e}(t)+Bu(t)-\bar{L}_{D1}\bar{C}\dot{\bar{e}}(t)+\bar{L}_{S1}u_S(t) \tag{23}$$

其中：$\bar{L}_{P1}$、$\bar{L}_{D1}$ 和$\bar{L}_{S1}$ 分别为$\bar{L}_P$、$\bar{L}_D$ 和$\bar{L}_S$ 的前 3 项。

构造如下积分滑模面：

$$S_x(t)=G\hat{x}(t)-\int_0^t G(A+BK)\hat{x}(\theta)\mathrm{d}\theta \tag{24}$$

令 $G=B^{+}$。

所设计的控制器为：

$$\begin{cases} u(t)=K\hat{x}(t)-lS_x(t)-\sigma(t)\mathrm{sat}(S_x(t)) \\ \mathrm{sat}(S_x(t))=\begin{cases} \dfrac{S_x(t)}{\alpha}, & \|S_x(t)\|\leqslant\alpha \\ \mathrm{sign}(S_x(t)), & \|S_x(t)\|>\alpha \end{cases} \end{cases} \tag{25}$$

其中，$\sigma(t)=-\lambda(t)-\gamma+\rho+d$，$\lambda(t)=\|B^{+}\bar{L}_{P1}\bar{C}\bar{e}(t)\|$，$\alpha>0$。

下面验证设计的积分滑模容侵控制器的稳定性。

定理 2 在微电网受到虚假数据注入攻击下，如果非奇异矩阵 $P\in R^{4\times4}>0$，$Y\in R^{4\times4}>0$ 和 $U\in R^{4\times4}>0$ 使得如下约束成立：

$$\begin{cases} P\bar{S}^{-1}\bar{A}-Y\bar{C}+(P\bar{S}^{-1}\bar{A}-Y\bar{C})^{T}<0 \\ \bar{B}_1^{T}\bar{S}^{-T}P=U\bar{C} \end{cases} \tag{26}$$

则积分滑模控制器式(25)可保证系统渐近稳定。

这表明：在准确估计出攻击信息后，通过所提出的积分滑模容侵控制器可以使孤岛交流微电网控制系统在受到虚假数据注入攻击时仍然保持渐进稳定性。

## 3 仿真验证

为了验证本文所提出的主动容侵方法可以确保微电网系统在受到虚假数据注入攻击时的稳定性，将通过以下的仿真实验进行研究验证。

由式(2)孤岛交流微电网逆变系统模型设定：$A=\begin{bmatrix} -80 & 40 & -2\,000 \\ 40 & -80 & 2\,000 \\ 10\,000 & -10\,000 & 0 \end{bmatrix}$，$B=\begin{bmatrix} 2\,000 \\ 0 \\ 0 \end{bmatrix}$，$C=[1\ \ 1\ \ 0]$。

定义 $d=0.5$，$\rho=1$。

(1)在所设计的滑模观测器中，令：

$$\bar{L}_D=[0\ \ 0\ \ 0\ \ 0.1]^{T} \tag{27}$$

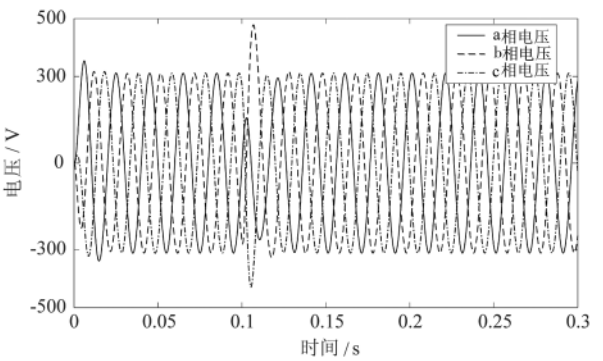
由$\bar{S}=E+\bar{L}_D\bar{C}$可以得到：

$$\bar{S}=\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0.1 & 0.1 & 0 & 0.1 \end{bmatrix} \tag{28}$$

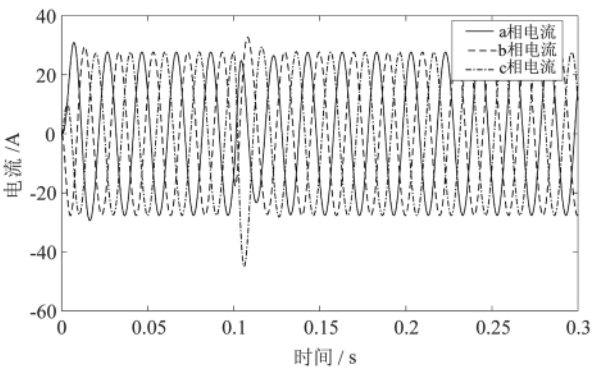
$\bar{S}$为可逆矩阵，在观测器滑模输入项中，由定理 1 利用 MATLAB/LMI 工具箱算出$\bar{L}_P=[52.1\ \ -0.2\ \ 103.8\ \ -20.1]^{T}$。

(2)在积分滑模容侵控制器中，根据定理 2 仿真得到 $K=[49.24\ \ -15.88\ \ -54.32]$。

假设微电网系统在 0.1 s 时检测的传感器侧受到了常值虚假数据注入攻击，即 $f_{a1}=2$，此时输出的电压和电流的仿真图如图 3 所示。假设微电网系统在 0.1 s 时检



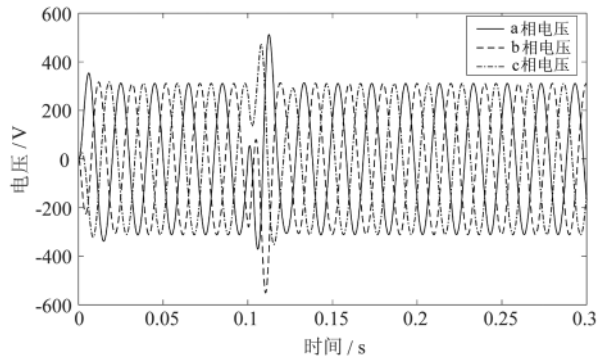

(a)输出电压波形图



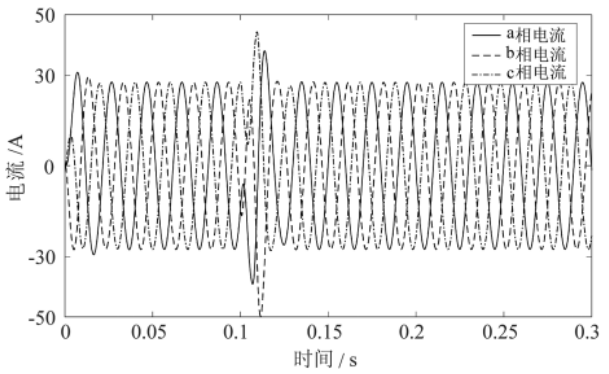

(b)输出电流波形图

图 3 检测 $i_1$ 的传感器侧受到攻击时输出电压、电流波形图

测 $u_C$ 的传感器侧受到了虚假数据注入攻击，即 $f_{a3}=3$，此时输出的电压和电流的仿真图如图 4 所示。在 0.1 s 时检测 $i_1$ 的传感器侧受到常值的虚假数据注入攻击，即 $f_{a1}=2$ 且在 0.2 s 时检测 $u_C$ 的传感器侧受到常值的虚假数据注入攻击，即 $f_{a3}=3$，此时输出的电压和电流的仿真图如图 5 所示。




(a)输出电压波形图



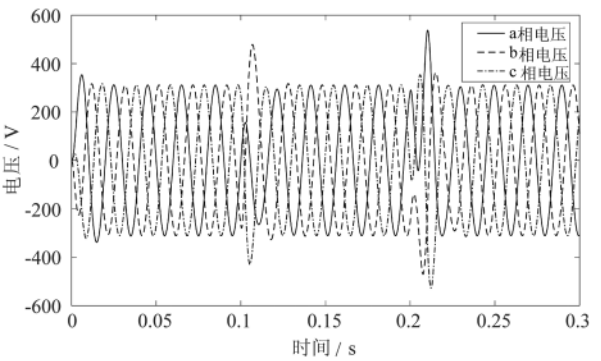

(b)输出电流波形图

图 4　检测 $u_C$ 的传感器侧受到攻击时输出电压、电流波形图

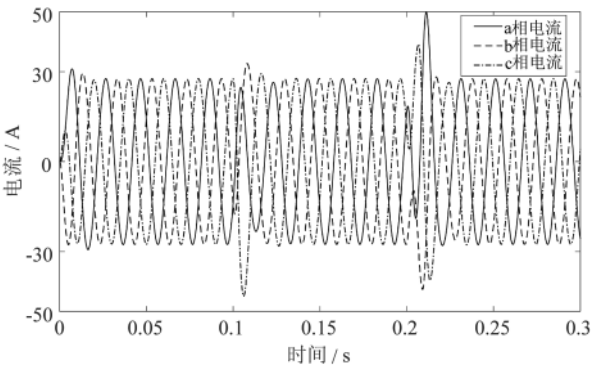
图 3、图 4 和图 5 为不同时间检测不同的电流和电压的传感器侧受到虚假数据注入攻击时使用本文提出的主动 $H_\infty$ 容侵方法后输出的电压和电流波形图，可以看出电压和电流在受到虚假数据注入攻击时都发生了突变。由于加入了容侵控制器，电压和电流逐渐回到了稳定运行时的电压和电流值。这就证明本文所设计的容侵控制器不仅具有良好的扰动抑制性能，而且有良好的攻击容侵的能力。

## 4 结论

本文针对微电网系统中难以避免的虚假数据注入攻击问题，设计滑模观测器对攻击进行检测和系统输出量观测，利用 LMI 方法简化观测器参数选取过程。此外，还提出了基于观测的主动容侵控制算法，利用积分滑模容侵控制器对攻击进行容侵控制。通过 MATLAB/Simulink 对微电网系统数学模型进行仿真验证，验证了所提出方案的可行性和有效性。从仿真结果可以看出：针对虚假数据注入攻击问题所提出的主动容侵控制策略，由于滑




(a)输出电压波形图




(b)输出电流波形图

图 5　检测 $i_2$ 和检测 $u_C$ 的传感器侧在不同时间受到攻击时输出电压、电流波形图

模观测器的存在能有效识别攻击并且在攻击发生时保持观测器系统稳定，基于观测的积分滑模容侵控制器能及时抑制 FDIA 对系统的影响，保证了系统的稳定性和可靠性。

## 参考文献

[1] 叶夏明.电力信息物理系统通信网络性能分析及网络安全评估[D].杭州：浙江大学，2015.

[2] 陈郁林.抵御虚假数据注入攻击的微电网分布式二次控制策略研究[D].杭州：浙江大学，2021.

[3] HAHN A，GOVINDARASU M.Cyber attack exposure evaluation framework for the smart grid[J].IEEE Transactions on Smart Grid，2011，2(4)：835-843.

[4] TIAN J，WANG B，XIA L I.State-preserving topology attacks and its impact on economic operation of smart grid[J].Power System Protection and Control，2018，46(1)：50-56.

[5] 王勇，武津园，陈雪鸿，等.基于卡尔曼滤波的电力虚假数据注入攻击检测方法[J].上海电力大学学报，2021，37(2)：205-210.

[6] 俞晓天，朱俊威，冯宇.针对一类非线性系统的虚假数据注入攻击估计方法[J].小型微型计算机系统，2020，41(11)：2407-2412.

[7] 曾俊娆，李鹏，高莲，等.基于 TNPE 的智能电网虚假数据

(下转第 99 页)

给 p1 赋值为 TRUE，也不能再达到状态 State_1 了。

## 5 结论

本文完成对 ST 语言和 LD 语言生成有限状态机图的分析，在语言分析的基础上基于有限状态机实现了模型描述语言和模型检测的研究。在完成图形化建模编程后，可以在编译阶段对建立的模型进行检查，对模型中的不一致、类型不匹配、数据回路等所有的模型错误进行定位，以便实现对工程逻辑的纠错。

## 参考文献

[1] ISO/IEC.ISO/IEC 27000 family-information security management systems[S].2018.

[2] 张文博，陈思敏，魏立斐，等.基于形式化方法的智能合约验证研究综述[J].网络与信息安全学报，2022，8(4)：12-28.

[3] 肖思慧，刘琦，黄滟鸿，等.基于 SysML 的机载软件分层精化建模与验证方法[J].软件学报，2022，33(8)：2851-2874.

[4] 毛侠.面向可编程逻辑控制器的功能安全形式化建模与验证方法研究[D].上海：华东师范大学，2022.

[5] 范宝文，包健.嵌入式控制系统时序安全性建模及验证[J].杭州电子科技大学学报(自然科学版)，2021，41(6)：21-27.

[6] 李建龙.PLC 系统及其 FBD 编程语言的形式化建模与实时性验证[D].泉州：华侨大学，2015.

[7] 卜祥兴.符合工控 IEC 61131-3 国际标准的结构化文本程序的验证方法研究[D].上海：华东师范大学，2018.

[8] CIMATTI A，CLARKE E，GIUNCHIGLIA E，et al.NuSMV 2：an opensource tool for symbolic model checking[C]//International Conference on Computer Aided Verification，2002：359-364.

[9] 李乾旭.基于 NuSMV 的 XX 软件需求模型转换与形式化验证[D].北京：北京交通大学，2021.

[10] 刘畅，蒋永平，马春燕，等.基于 NuSMV 的 AADL 模型形式化验证技术[J].航空学报，2022，43(3)：451-466.

[11] 邓刘梦，葛晓瑜，宛伟健.基于 NuSMV 的 SysML 模型形式化验证[J].计算机技术与发展，2019，29(10)：153-156.

(收稿日期：2021-11-04)

作者简介：

郭肖旺(1986-)，女，硕士，高级工程师，主要研究方向：工业软件、编译技术。

赵德政(1985-)，男，博士，研究员，主要研究方向：工业自动化控制、工控安全。

扫码下载电子文档

(上接第 93 页)

注入攻击检测[J].中国安全生产科学技术，2021，17(3)：124-129.

[8] 阮兆文，孟干，周冬青，等.智能电网中的虚假数据注入攻击检测方法研究[J].自动化与仪器仪表，2019(3)：49-52.

[9] 彭华晔，彭晨，孙洪涛，等.微电网在虚假数据注入攻击下的增量检测机制[J].信息与控制，2019，48(5)：522-527.

[10] HAO J，KANG E，SUN J，et al.An adaptive Markov strategy for defending smart grid false data injection from malicious attackers[J].IEEE Transactions on Smart Grid，2016，4(6)：1-3.

[11] YANG X，ZHAO P，ZHANG X，et al.A Gaussian-mixture model based detection scheme against data integrity attacks in the smart grid[J].IEEE Internet of Things Journal，2016，82(5)：1-6.

[12] WANG H，RUAN J，WANG G，et al.Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks[J].IEEE Transactions on Industrial Informatics，2018，56(2)：82-86.

[13] 张逸为，许德智，杨玮林，等.含混合储能的互联电力系统传感器容错负荷频率控制[J].控制与决策，2021，36(5)：9-10.

[14] 安娜.微电网模式切换控制策略研究[D].秦皇岛：燕山大学，2014.

[15] 游国栋，李继生，侯勇，等.光伏 LCL 型并网逆变器的积分滑模容错控制策略[J].太阳能学报，2018，39(4)：1008-1017.

(收稿日期：2021-11-19)

作者简介：

王君(1973-)，女，博士，教授，主要研究方向：动态系统故障诊断与容错控制。

冯甜(1993-)，通信作者，女，硕士，主要研究方向：动态系统故障诊断与容错控制，E-mail：2691978497@qq.com。

扫码下载电子文档

# 版权声明