目录
CONTENTS

东北电力大学 NORTHEAST ELECTRIC POWER UNIVERSITY

CSCT NEEPU Cyber Security Control Team

Dynamic load altering attack detection for cyber physical power systems via sliding mode observer

(International Journal of Electrical Power and Energy Systems)

作者：李健 李泓良 苏庆宇

1.1 动态负载攻击

动态负载改变攻击是一种利用电网负载的攻击。攻击路径如图1所示。动态负载改变攻击不断推移控制和调整攻击的特性使得这种攻击能使得初始冲击引起的波动逐渐扩大，系统极点移动，直到系统不稳定。

而目前的研究中少有对动态负载改变攻击的检测研究。

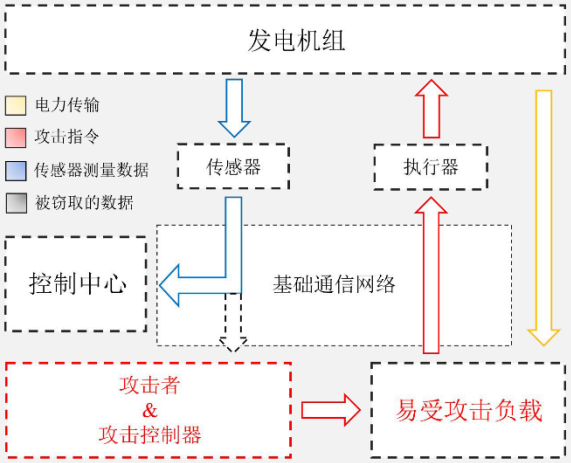

图1. 动态负载改变攻击一般攻击路径

CSCT NEEPU Cyber Security Control Team | 研究意义及现状 | 研究技术路线 | 数学模型推导及仿真模型搭建 | 仿真及半实物仿真验证 | 作者简介

2.1 研究技术路线

01数学模型

考虑用发电机转子摆动方程和系统直流潮流方程来建立电力系统小信号数学模型。

考虑动态负载改变攻击能通过反馈调整攻击的特点，通过PI控制器来建立闭环攻击模型。

02检测方案

设计反正切滑模观测器，并用H∞性能指标来约束求解观测器增益矩阵，以减小系统中攻击和干扰造成的影响。

设计攻击检测逻辑检测观测器输出信号中是否存在攻击。

03仿真验证

以三机九节点电力系统为例：

先在MATLAB/Simulink平台上进行仿真验证。

而后，在远宽StarSim硬件在环仿真实验平台进行仿真验证。

3.1 电力系统模型

考虑发电机转子摆动方程和系统直流潮流方程来描述系统。考虑一个具有n个发电机和m个负载总线的电力系统。

- 系统潮流方程描述为:

$$P_{Gi} = \sum_{j\in G} Y_{ij}(\delta_i - \delta j) + \sum_{j\in M} Y_{ij}(\delta_i - \theta j), \forall i \in G$$

$$P_{Li} = -\left(\sum_{i\in G} Y_{ij}(\theta_i - \delta j) + \sum_{i\in M} Y_{ij}(\theta_i - \theta j)\right), \forall i \in L$$

- 发电机转子摆动方程描述为:

$$\dot{\delta}_i = \omega_i$$
$$M_{gi}\dot{\omega}_i = P_{Mi} - D_{gi}\omega_i - P_{Gi}$$

CSCT NEEPU Cyber Security Control Team | 研究意义及现状 | 研究技术路线 | 数学模型推导及仿真模型搭建 | 仿真及半实物仿真验证 | 作者简介

3.1 电力系统模型

对于机械输入功率P_{Mi}，假设其受到负载频率控制器和涡轮机调速器控制器的影响。这两个控制器可以建模为以下比例积分PI控制器：

$$P_{Mi} = -\left(K_{Pi}\omega_i + K_{Ii}\int_0^t \omega_i\right)$$

其中:$K_P > 0$是比例控制器系数矩阵，$K_I > 0$是积分控制器系数矩阵。

基于上述方程，电力系统状态空间模型可以被总结为：

$$\dot{x}(t) = Ax(t) + Bu(t)$$
$$y(t) = Cx(t)$$

其中系统矩阵$A = \begin{bmatrix} 0 & I \\ M_g^{-1}\left(L_{gl}L_{ll}^{-1}L_{lg} - L_{gg}\right) & -M_g^{-1}D_g \end{bmatrix} \in \mathbb{R}^{2n\times 2n}$，输入矩阵$B = \begin{bmatrix} 0 \\ M_g^{-1} \end{bmatrix} \in \mathbb{R}^{2n\times n}$。

3.2 攻击模型

如图2所示，DLAA可以分为开换DLAA和闭环DLAA。

- 开环DLAA：攻击者缺乏或不具备从电网获取数据的方法。攻击者主要使用历史数据提前设计攻击轨迹。
- 闭环DLAA：攻击者可以监控系统，从而获得大段或者实时的系统状态数据。例如通过安装传感器或侵入网络基础设施，并且根据所获得的有效信息设计含有状态反馈的攻击轨迹。

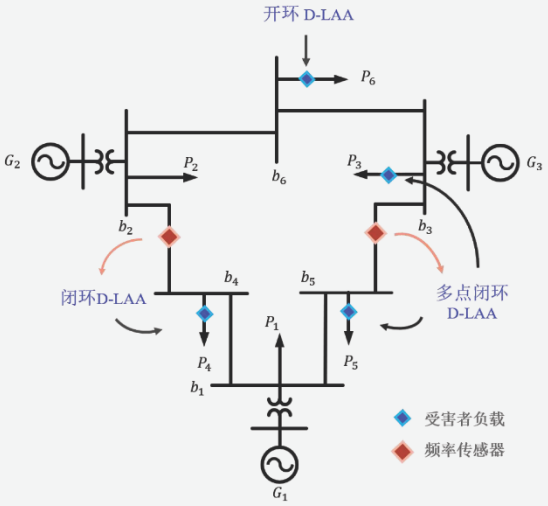

图2. 三机九节点系统和DLAA类型

3.2 攻击模型

在闭环攻击的情况下，攻击者可能会使用反馈控制器，如bang–bang、P、PI、PID控制器作为攻击手段。通过反馈攻击，导致系统极点移动，最终可能引起系统震荡。攻击导致的极点移动如图3所示。

假设攻击来自比例控制器，动态负载改变攻击建模为：

$$\eta_L(t) = -K_{vs}^{L} w(t)$$

其中：$v \epsilon M$是受害者母线，$-K_{vs}^{L} < 0$是攻击控制器增益。

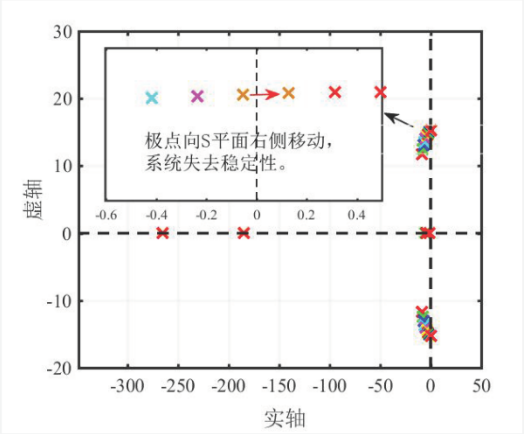

图3. DLAA下的极点图

3.3 系统模型+攻击模型

由于攻击是由攻击者调控可控负载产生的，结合攻击建模的负载需求功率$P_L(t)$可以重写为:

$$P_L(t) = P_{Ls}(t) + \eta_L(t) + \Delta_L(t)$$

其中: $P_{Ls}(t)$是负载需求功率的安全部分，$\eta_L(t)$是动态负载改变攻击，$\Delta_L(t)$表示负载侧波动。

最终，受到动态负载改变攻击攻击的电力系统被描述为:

$$\dot{x}(t) = Ax(t) + BP_{Ls}(t) + B\Delta_L(t) + B\eta_L(t)$$
$$y(t) = Cx(t)$$

CSCT NEEPU Cyber Security Control Team | 研究意义及现状 | 研究技术路线 | 数学模型推导及仿真模型搭建 | 仿真及半实物仿真验证 | 作者简介

3.4 滑模观测器

首先，通过使用带有反正切滑模项的观测器来估计系统中由攻击和干扰等因素所引起的偏差信号。观测器设计如下:

$$\dot{\hat{x}}(t) = A\hat{x}(t) + BP_{Ls}(t) + L\big(y(t) - \hat{y}(t)\big) + B_v v(t)$$
$$\hat{y}(t) = C\hat{x}(t)$$

其中: $\hat{x}(t)$是状态估计，$\hat{y}(t)$是输出估计，$v(t) = Garcran(y(t) - \hat{y}(t))$是反正切滑模项。

观测器误差系统如下:

$$\dot{e}(t) = (A - LC)e(t) + B\eta_L(t) + B\Delta_L(t) - B_v \mathrm{Garctan}(Ce(t))$$

其中: $e(t) = x(t) - \hat{x}(t)$是状态估计误差，$r(t) = e_y(t) = y(t) - \hat{y}(t)$是输出估计误差。

3.4 滑模观测器

考虑到攻击对误差系统和偏差信号的影响，给出如下H_∞性能指标:

$$\int_0^\infty r^T(t)r(t) < \gamma^2\eta_L^T(t)\eta_L(t)dt$$

其中γ是一个常数。

结合上述指标，有如下不等式满足时，则误差系统稳定:

$$\Psi = \int_0^t r^T(\phi)r(\phi) - \gamma^2\eta_L^T(\phi)\eta_L(\phi) + \dot{V}(\phi)\,d\phi - V(\phi)$$
$$\leq \int_0^t r^T(\phi)r(\phi) - \gamma^2\eta_L^T(\phi)\eta_L(\phi) + \dot{V}(\phi)\,d\phi$$

3.4 滑模观测器

对上式变换有:

$$\underbrace{\begin{bmatrix}(A-LC)^T & B^T\\ I & 0\\ 0 & I\end{bmatrix}^T}_{N_Y^T}\underbrace{\begin{bmatrix}0 & P & 0\\ P & C^TC+PBB^TP & 0\\ 0 & 0 & -\gamma^2 I\end{bmatrix}}_{\lambda}\underbrace{\begin{bmatrix}(A-LC) & B\\ I & 0\\ 0 & I\end{bmatrix}}_{N_Y}<0 \text{ 和 } \underbrace{\begin{bmatrix}0\\0\\I\end{bmatrix}^T}_{N_\Sigma^T}\underbrace{\begin{bmatrix}0 & P & 0\\ P & C^TC+PBB^TP & 0\\ 0 & 0 & -\gamma^2 I\end{bmatrix}}_{\lambda}\underbrace{\begin{bmatrix}0\\0\\I\end{bmatrix}}_{N_\Sigma}=-\gamma^2 I<0$$

根据上面的两个不等式，用投影定理得到如下不等式:

$$\lambda + He\left(\underbrace{\begin{bmatrix}-I\\(A-LC)^T\\B^T\end{bmatrix}}_{Y^T}\underbrace{\begin{bmatrix}F & aF & 0\end{bmatrix}}_{\Sigma}\right)<0，\text{最终变为:}\begin{bmatrix}-He(F) & P-\alpha F+F^TA-\zeta C & F^TB & 0\\ * & C^TC+\alpha He(F^TA-\zeta C) & \alpha F^TB & PB\\ * & * & -\gamma^2 I & 0\\ * & * & * & -I\end{bmatrix}<0$$

该不等式通过MATLAB中的LMI工具包，可解得满足观测器稳定的增益矩阵。

3.5 攻击检测逻辑

得到满足误差系统收敛于零的增益矩阵后，根据误差系统有:

$$B\xi(t) = B(\eta_L(t) + \Delta_L(t)) + (\mathrm{A} - \mathrm{LC})e(t) - \dot{e}(t)$$

其中:$\xi(t)$是偏差信号。当误差系统(4-13)收敛于零时，$(\mathrm{A} - \mathrm{LC})e(t) - \dot{e}(t)$收敛于零。$\Delta_L(t)$是一个能量很小的自然波动。因此，偏差信号$\xi(t)$的变动主要由攻击$\eta_L(t)$所引起。

基于观测器所得到的偏差信号$\xi(t)$，攻击检测逻辑设计如下:

$$\begin{cases} |\xi_i(t)| > J_{th} \Rightarrow \text{系统遭遇到 DLAA} \\ |\xi_i(t)| \le J_{th} \Rightarrow \text{系统未遭遇到 DLAA} \end{cases}$$

其中:$\xi_i(t)$是第i个$\xi(t)$，J_{th}是检测阈值，$|\xi_i(t)|$是$\xi_i(t)$的绝对值。

4.1 MATLAB/Simulink仿真分析

给出三种不同的攻击案例以验证所提出检测方案的有效性。

情况 1: 单点闭环攻击，攻击控制矩阵$K_{12}^{L} = 5$，自然波动$\Delta_{L1} = 0.05$，$\Delta_{L2} = 0.07$，$\Delta_{L3} = 0.08$，$\Delta_{L4} = 0.09$，$\Delta_{L5} = 0.08$，$\Delta_{L6} = 0.04$。

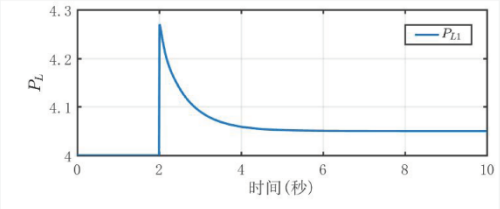

图4. Case1受攻击节点的负载变化

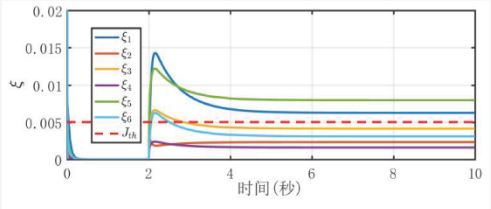

图5. Case1偏差信号及攻击检测

4.1 MATLAB/Simulink仿真分析

情况 2: 多点闭环攻击，攻击控制矩阵$K_{41}^{L}=2$，$K_{51}^{L}=2$。情况 3: 多点闭环攻击，但不同节点，攻击控制矩阵$K_{22}^{L}=4$，$K_{62}^{L}=4$。

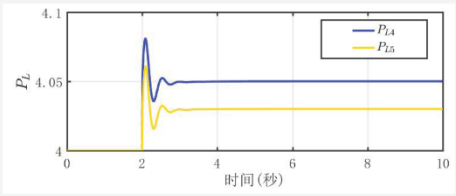

图6. Case2受攻击节点的负载变化

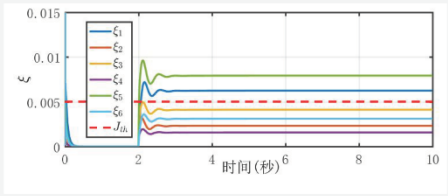

图7. Case2偏差信号及攻击检测

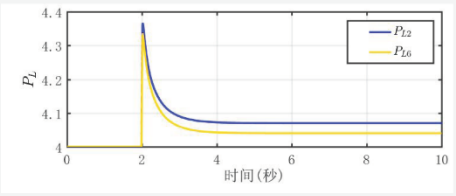

图8. Case3受攻击节点的负载变化

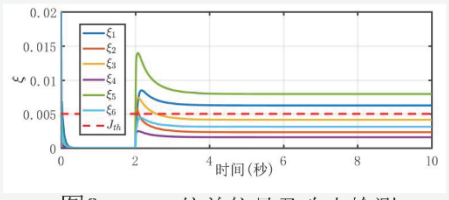

图9. Case3偏差信号及攻击检测

CSCT NEEPU Cyber Security Control Team | 研究意义及现状 | 研究技术路线 | 数学模型推导及仿真模型搭建 | 仿真及半实物仿真验证 | 作者简介

4.2 远宽能源StarSim硬件在环仿真平台

半实物仿真设备和结果如图10和11所示。

RCP: Rapid Control Prototype，由主机中的程序StarSim RCP驱动，主要负责运行主机PC输出的控制程序。

I/O Board:支持数据在各个设备之间的传输。

RTS: Real-time simulator，由软件StarSim HIL驱动。仿真程序能够通过Field-Programmable Gate Array (FPGA)实时仿真器运行。

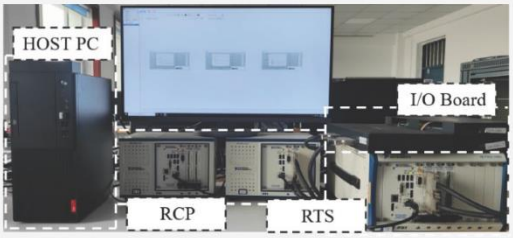

图11. 攻击检测半实物仿真

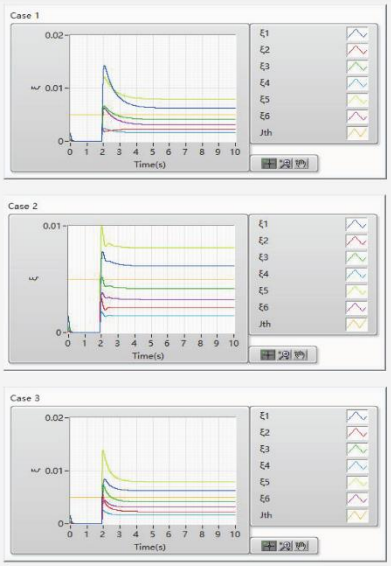

图11. 攻击检测半实物仿真

作者简介

李健，女，教授，博士生导师，研究方向为鲁棒控制、电力电子控制、故障检测技术及其在微电网中的应用。电话: 13844223038, 邮箱: lijian@neepu.edu.cn.

李泓良，男，硕士研究生，研究方向为电力信息物理系统网络攻击检测。电话: 13384325365, 邮箱: lihongliangstudy@163.com.

苏庆宇，男，教授，硕士生导师，研究方向为切换系统与混杂控制理论及其在电力系统中的应用。电话:13844233039,邮箱: suqingyu@neepu.edu.cn.