文章编号：1674－2869(2026)03－0335－08

电力信息物理系统中基于自适应卡尔曼滤波的动态负载变化攻击检测

张艾玲[1]，王后能*[1]，廖小兵[1]，叶石丰[2]
1. 武汉工程大学电气信息学院，湖北 武汉 430205；
2. 广东电网有限责任公司广州供电局，广东 广州 510620

摘　要：针对电力信息物理系统(CPPS)中负载端可能遭受动态负载变化攻击(D-LAA)的问题，分析了该攻击对电力系统运行产生的影响，并提出了基于状态估计器的攻击检测方法。首先以攻击者的视角基于比例积分控制器设计D-LAA，通过仿真验证了所提攻击模型能使受害负载的功率和发电机转子角频率产生更大的波动和偏移，且攻击用时更短。然后以防御者的视角设计状态估计器，针对卡尔曼滤波算法对噪声模型的统计性要求较高、攻击状态下估计误差增大的问题，设计了改进的自适应渐消因子卡尔曼滤波算法，该算法的渐消因子基于新息协方差估计值得到。最后基于状态估计结果提出攻击检测方法。仿真结果表明所提算法具有更高的估计精度和异常信号敏感度，检测方法能及时检测到攻击信号，为CPPS的安全稳定运行建立了防线。

关键词：电力信息物理系统；动态负载变化攻击；状态估计器；自适应卡尔曼滤波；攻击检测
中图分类号：TM743　　**文献标志码**：A　　**DOI**：10.19843/j.cnki.CN42-1779/TQ.202510004

Detection of dynamic load-altering attacks in cyber physical power system using adaptive Kalman filter

ZHANG Ailing[1], *WANG Houneng*[*1], *LIAO Xiaobing*[1], *YE Shifeng*[2]
1. School of Electrical and Information Engineering, Wuhan Institute of Technology, Wuhan 430205, China;
2. Guangzhou Power Supply Bureau of Guangdong Grid Co., Ltd, Guangzhou 510620, China

Abstract: Addressing the threat of dynamic load-altering attacks(D-LAA)on the load sides in cyber physical power systems(CPPS), in this paper we analyzed the impacts of such attacks on power system operation and proposed a detection method based on the state estimator. First, from the attacker's perspective, a D-LAA was designed using a proportional-integral controller. Simulations verified that the proposed attack model induced greater fluctuations and deviations in the victim load's power and the generator rotor frequencies, while also requiring less time to execute. Then, from the defender's perspective, a state estimator was designed. To overcome the limitations of the standard Kalman filter—specifically its high dependency on accurate noise statistics and increased estimation errors under attack conditions—an improved adaptive fading-factor Kalman filter algorithm was introduced. In this algorithm, the fading factor was derived from the estimated innovation covariance. Finally, an attack detection method was developed based on the state estimation results. Simulation results showed that the proposed algorithm achieved higher estimation accuracy

收稿日期：2025-10-14
基金项目：国家自然科学基金(52107122)；武汉工程大学研究生教育创新基金(CX2024567)
作者简介：张艾玲，硕士研究生。Email：895185946@qq.com
***通信作者**：王后能，博士，副教授。Email：wanghouneng@163.com
引文格式：张艾玲，王后能，廖小兵，等. 电力信息物理系统中基于自适应卡尔曼滤波的动态负载变化攻击检测[J]. 武汉工程大学学报，2026，48(3)：335-342.

of and greater sensitivity to abnormal signals, and the detection method could identify the attack signals promptly, thereby establishing a defensive barrier for the secure and stable operation of CPPS.

Keywords: cyber physical power system; dynamic load-altering attack; state estimator; adaptive Kalman filter; attack detection

信息物理系统(cyber physical system,CPS)是一种融合了物理系统、网络通信和计算机科学的新型智能系统[1]。现代电力系统作为典型的CPS,由基础电力网络和信息网络组建而成,是电力应用的关键核心和典型代表[2]。由系统的结构特点可知,电力信息物理系统(cyber physical power system,CPPS)主要面临来自通信通道和物理设备的安全威胁[3]。近年来,随着网络规模的扩张以及通信环境的开放,使得系统容易受到攻击[4]。拒绝服务攻击[5-6]、虚假数据注入攻击[7-9]、中间人攻击[10]都是常见的针对网络通道的攻击,攻击者在通信通道阻断或篡改数据使网络系统的功能被破坏,导致CPPS无法及时执行任务甚至崩溃。

传感器和控制器等物理设备作为与电力系统交互的重要部分,攻击者可以通过恶意篡改其工作逻辑,破坏数据的真实性,从而诱导电力系统做出错误响应。负载变化攻击(load altering attack,LAA)就是利用这些物理设备去改变电网中的某些不安全负载,使电能溢出或发电机卸载来破坏电力系统的稳定运行[11]。Mohsenian-Rad等[11]指出了易遭受LAA的两种负载类型,即不可控负载和频率响应负载,并以突然改变受损负载体积的方式研究了静态LAA。在此基础上,Amini等[12]以发电机转子角频率作为反馈设计了动态负载变化攻击(dynamic load altering attack,D-LAA),并基于比例(proportional,P)控制器设计了单点闭环D-LAA,不同于静态LAA仅改变受损负载的体积,D-LAA还会改变负载的轨迹。Amini等[13]进一步分析了D-LAA的工作原理及其造成智能电网不稳定的条件,但只针对攻击造成发电机卸载的情况进行了分析,而没有考虑使系统产生额外功率的情况。

状态估计是当代电力系统中能量管理的重要组成部分,是实现CPPS安全稳定运行的基础[14]。卡尔曼滤波器(Kalman filter,KF)通过含有高斯噪声的输入输出观测数据,对系统状态进行最优估计,被广泛应用于航空领域的导航[15]、轨迹预测[16]和姿态估计[17]以及工业过程的状态监测和故障诊断。但是,当噪声模型难以确定、输入信号发生突变时,KF的估计精度、鲁棒性以及收敛速度均表现较差。自适应渐消因子卡尔曼滤波器(adaptive fading factor Kalman filter,AFFKF)通过引入渐消因子来调整先验状态误差协方差矩阵,可以有效解决该问题。Li等[18]提出了基于新息协方差的卡尔曼滤波算法,通过新息序列的协方差理论值构造函数来求取渐消因子,并根据状态向量估计值和状态向量预测值之间的差异进行D-LAA检测。但是当模型不准确时,基于内部模型计算的新息协方差理论值无法反映系统的实际运行状况,从而使状态估计结果偏离实际值。

为加剧D-LAA对电力系统安全稳定运行的破坏,本文基于比例积分(proportional integral,PI)控制器设计D-LAA,在2个场景中研究其对系统负载功率和发电机角频率产生的影响。为进一步提高状态估计器的准确性,设计了基于新息协方差估计值的AFFKF,其中新息协方差估计值基于渐消记忆指数加权计算,最后结合欧几里得距离和残差函数设计攻击检测方法,实现D-LAA检测。数值仿真表明,本文所提的基于PI控制器的攻击模型能对系统的稳定性造成更大的破坏,所提的改进AFFKF算法具有更好的状态估计精度和异常信号敏感度。

1 系统模型

1.1 电力系统模型

考虑一个以N为总线的电力系统,其中发电机总线集合用$G=\{g_1,g_2,\cdots,g_n\}$表示,负载总线集合用$L=\{l_1,l_2,\cdots,l_m\}$表示,g_n和l_m分别表示第n条发电机总线和第m条负载总线,故该电力系统的潮流方程可写成:

$$\begin{cases} P_i^{\mathrm{G}}=\sum\limits_{j\in G}J_{ij}\left(\delta_i-\delta_j\right)+\sum\limits_{j\in L}J_{ij}\left(\delta_i-\theta_j\right) & \forall i\in G \\ -P_i^{\mathrm{L}}=\sum\limits_{j\in G}J_{ij}\left(\theta_i-\delta_j\right)+\sum\limits_{j\in L}J_{ij}\left(\theta_i-\theta_j\right) & \forall i\in L \end{cases} \tag{1}$$

式(1)中:P_i^{G}代表发电机在第i条总线处注入的功率;P_i^{L}代表负载在第i条总线处消耗的功率;δ_i为第i条总线处的发电机相角;θ_i为第i条总线处的电压相角;J_{ij}则表示第i条总线和第j条总线之间的线路导纳,若二者之间无传输线路连接,则$J_{ij}=0$。

根据摆动方程对发电机进行建模:

$$\begin{cases}\dot{\delta}_i = \omega_i \\ M_i\dot{\omega}_i = P_i^{\text{in}} - d_i\omega_i - P_i^{\text{G}}\end{cases} \tag{2}$$

式(2)中：ω_i是转子角频率相对于标准角频率的偏差，M_i是转子惯量，P_i^{in}是机械输入功率，d_i是阻尼系数。

现实中P_i^{in}易受涡轮调速控制器和负载频率控制器的影响，为了简化分析过程本文暂不考虑发电机的时滞性和其他内部因素。故上述两种控制器可统一抽象为PI控制器的形式，发电机的机械输入功率可表示为：

$$P_i^{\text{in}} = K_i^{\text{P}}\omega_i + K_i^{\text{I}}\int_0^t \omega_i = K_i^{\text{P}}\omega_i + K_i^{\text{I}}\delta_i \tag{3}$$

式(3)中：K_i^{P}和K_i^{I}分别表示积分控制器系数和比例控制器系数。

将式(1)和式(3)代入式(2)可得：

$$M_i\dot{\omega}_i = (K_i^{\text{P}} - d_i)\omega_i + K_i^{\text{I}}\delta_i - \sum_{j\in G} J_{ij}\left(\delta_i - \delta_j\right) - \sum_{j\in L} J_{ij}\left(\delta_i - \delta_j\right) \tag{4}$$

消除负载总线处电压相角的影响，系统状态空间模型可以描述为：

$$\begin{bmatrix}\dot{\boldsymbol{\delta}}(t)\\ \dot{\boldsymbol{\omega}}(t)\end{bmatrix} = \begin{bmatrix}\boldsymbol{0} & \boldsymbol{I}\\ \boldsymbol{M}^{-1}\left[\boldsymbol{K}^{\text{I}} - \boldsymbol{J}^{\text{GG}} + \boldsymbol{J}^{\text{GL}}\left(\boldsymbol{J}^{\text{LL}}\right)^{-1}\boldsymbol{J}^{\text{LG}}\right] & \boldsymbol{M}^{-1}\left(\boldsymbol{K}^{\text{P}} - \boldsymbol{D}\right)\end{bmatrix}\begin{bmatrix}\boldsymbol{\delta}(t)\\ \boldsymbol{\omega}(t)\end{bmatrix} + \begin{bmatrix}\boldsymbol{0}\\ \boldsymbol{M}^{-1}\boldsymbol{J}^{\text{GL}}\left(\boldsymbol{J}^{\text{LL}}\right)^{-1}\end{bmatrix}\boldsymbol{P}^{\text{L}}(t) \tag{5}$$

式(5)中：t表示连续系统时间，$\boldsymbol{\delta}(t)$是发电机相角δ_i的向量集合，$\boldsymbol{\omega}(t)$是发电机转子角频率相对于标准角频率的偏差ω_i的向量集合，$\boldsymbol{J}^{\text{GG}}$是发电机总线间导纳的矩阵，$\boldsymbol{J}^{\text{GL}}$是发电机和负载总线间导纳的矩阵，$\boldsymbol{J}^{\text{LG}}$是负载和发电机总线间导纳的矩阵，$\boldsymbol{J}^{\text{LL}}$是负载总线间导纳的矩阵，$\boldsymbol{P}^{\text{L}}(t)$是负载消耗的功率$P_i^{\text{L}}$的向量集合，$\boldsymbol{K}^{\text{P}}$和$\boldsymbol{K}^{\text{I}}$分别为比例控制器系数和积分控制器系数的对角矩阵，$\boldsymbol{M}$和$\boldsymbol{D}$分别为发电机惯性系数和阻尼系数的对角矩阵，$\boldsymbol{I}$表示单位矩阵。

令$\boldsymbol{x}(t) = \left[\boldsymbol{\delta}^{\text{T}}(t)\quad \boldsymbol{\omega}^{\text{T}}(t)\right]^{\text{T}}$，$\boldsymbol{u}(t) = \boldsymbol{P}^{\text{L}}(t)$，并考虑噪声对系统的影响，则系统模型可以表示为：

$$\begin{cases}\dot{\boldsymbol{x}}(t) = \check{\boldsymbol{A}}\boldsymbol{x}(t) + \check{\boldsymbol{B}}\boldsymbol{u}(t) + \boldsymbol{w}(t)\\ \boldsymbol{y}(t) = \check{\boldsymbol{H}}\boldsymbol{x}(t) + \boldsymbol{v}(t)\end{cases} \tag{6}$$

式(6)中：$\boldsymbol{x}(t)$为系统状态向量，$\boldsymbol{y}(t)$为系统测量输出向量，$\boldsymbol{u}(t)$为系统输入向量，$\check{\boldsymbol{A}}$为状态转移矩阵且$\check{\boldsymbol{A}} = \begin{bmatrix}\boldsymbol{0} & \boldsymbol{I}\\ \boldsymbol{M}^{-1}\left[\boldsymbol{K}^{\text{I}} - \boldsymbol{J}^{\text{GG}} + \boldsymbol{J}^{\text{GL}}\left(\boldsymbol{J}^{\text{LL}}\right)^{-1}\boldsymbol{J}^{\text{LG}}\right] & \boldsymbol{M}^{-1}\left(\boldsymbol{K}^{\text{P}} - \boldsymbol{D}\right)\end{bmatrix}$，$\check{\boldsymbol{B}}$为输入矩阵且$\check{\boldsymbol{B}} = \begin{bmatrix}\boldsymbol{0}\\ \boldsymbol{M}^{-1}\boldsymbol{J}^{\text{GL}}\left(\boldsymbol{J}^{\text{LL}}\right)^{-1}\end{bmatrix}$，$\check{\boldsymbol{H}}$为连续系统下的测量矩阵，$\boldsymbol{w}(t)$和$\boldsymbol{v}(t)$分别为测量噪声向量和过程噪声向量。

1.2　动态负载变化攻击模型

假设攻击者以发电机转子角频率作为反馈信号控制负载功率P_i^{L}，发电机转子角频率通过攻击者提前部署的传感器获得，该传感器位于发电机总线s上。以PI控制器的形式在受害总线α处实施D-LAA，攻击序列$\boldsymbol{F}_\alpha(t)$可表示为：

$$\boldsymbol{F}_\alpha(t) = -\boldsymbol{K}_{\text{I},\alpha s}^{\text{L}}\int_0^t \boldsymbol{\omega}_s(t) - \boldsymbol{K}_{\text{P},\alpha s}^{\text{L}}\boldsymbol{\omega}_s(t) + \boldsymbol{f}_\alpha^{\text{L}} \tag{7}$$

式(7)中：$\boldsymbol{K}_{\text{I},\alpha s}^{\text{L}}$为攻击积分控制器增益，$\boldsymbol{K}_{\text{P},\alpha s}^{\text{L}}$为攻击比例控制器增益，$\boldsymbol{\omega}_s(t)$为发电机总线$s$上的发电机转子角频率相对于标称值的偏差的向量集合，$\boldsymbol{f}_\alpha^{\text{L}}$为攻击前生成的一个轻微频率偏差。

故受到D-LAA时CPPS的线性离散化模型为：

$$\begin{aligned}\boldsymbol{x}(k) &= \boldsymbol{A}\boldsymbol{x}(k-1) + \boldsymbol{B}\bar{\boldsymbol{u}}(k) + \boldsymbol{w}(k)\\ \boldsymbol{y}(k) &= \boldsymbol{H}\boldsymbol{x}(k) + \boldsymbol{v}(k)\end{aligned} \tag{8}$$

式(8)中：k表示离散系统时间；状态转移矩阵$\boldsymbol{A} \approx T\check{\boldsymbol{A}} + \boldsymbol{I}$，$T$为离散系统的采样周期；输入矩阵$\boldsymbol{B} \approx T\check{\boldsymbol{B}}$；$\boldsymbol{H}$为离散系统下的测量矩阵；$\boldsymbol{w}(k)$和$\boldsymbol{v}(k)$相互独立，且满足$\boldsymbol{w}(k) \sim N\left(0, \boldsymbol{Q}(k)\right)$、$\boldsymbol{v}(k) \sim N\left(0, \boldsymbol{R}(k)\right)$，$\boldsymbol{Q}(k)$为非负的过程噪声协方差矩阵，$\boldsymbol{R}(k)$为正定的测量噪声协方差矩阵；$\bar{\boldsymbol{u}}(k)$为攻击状态下的系统输入且$\bar{\boldsymbol{u}}(k) = \boldsymbol{P}^{\text{L}}(k) + \boldsymbol{F}_\alpha(k)$。

2　D-LAA检测

图1是CPPS中的D-LAA攻击检测方案。假设攻击者入侵了传感器并对电网数据进行实时监控，基于上述电网数据组成的系统输出测量值$\boldsymbol{y}(k)$，攻击者在控制器处发动了攻击，通过更改控制信号$\boldsymbol{u}(k)$使执行器发出了错误的工作指令，从

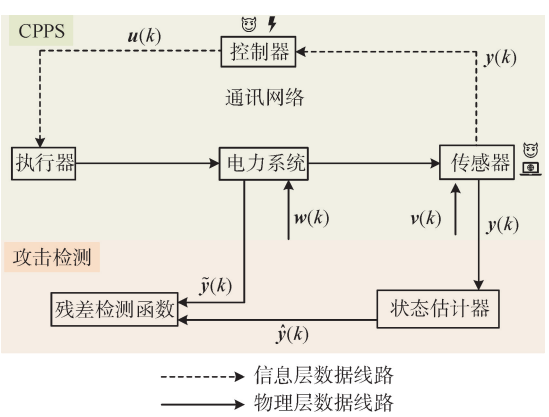

图1　CPPS中的D-LAA攻击检测方案

Fig. 1　D-LAA attack detection scheme in CPPS

而使电力系统的稳定性被破坏。检测部分则利用系统输出测量值$\boldsymbol{y}(k)$基于AFFKF算法设计状态估计器,然后基于系统输出估计值$\hat{\boldsymbol{y}}(k)$和系统输出实际值$\tilde{\boldsymbol{y}}(k)$之间的残差实现攻击检测。

2.1 状态估计器设计

根据KF算法,状态估计器的设计如下:

$$\hat{\boldsymbol{x}}(k|k-1)=\boldsymbol{A}\hat{\boldsymbol{x}}(k-1|k-1)+\boldsymbol{B}\boldsymbol{u}(k) \tag{9}$$

$$\boldsymbol{\varepsilon}(k)=\boldsymbol{y}(k)-\boldsymbol{H}\hat{\boldsymbol{x}}(k|k-1) \tag{10}$$

$$\boldsymbol{P}(k|k-1)=\boldsymbol{A}\boldsymbol{P}(k-1|k-1)\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{Q}(k) \tag{11}$$

$$\boldsymbol{K}(k)=\frac{\boldsymbol{P}(k|k-1)\boldsymbol{H}^{\mathrm{T}}}{\boldsymbol{H}\boldsymbol{P}(k|k-1)\boldsymbol{H}^{\mathrm{T}}+\boldsymbol{R}(k)} \tag{12}$$

$$\hat{\boldsymbol{x}}(k|k)=\hat{\boldsymbol{x}}(k|k-1)+\boldsymbol{K}(k)\boldsymbol{\varepsilon}(k) \tag{13}$$

$$\boldsymbol{P}(k|k)=(\boldsymbol{I}-\boldsymbol{K}(k)\boldsymbol{H})\boldsymbol{P}(k|k-1) \tag{14}$$

式(9)-式(14)中:$\hat{\boldsymbol{x}}(k|k-1)$为当前时刻的先验状态估计值,$\hat{\boldsymbol{x}}(k-1|k-1)$为上一时刻的后验状态估计值,$\boldsymbol{\varepsilon}(k)$表示当前时刻的新息向量,$\boldsymbol{P}(k|k-1)$为当前时刻的先验状态误差协方差矩阵,$\boldsymbol{P}(k-1|k-1)$为上一时刻的后验状态误差协方差矩阵,$\boldsymbol{K}(k)$表示当前时刻的卡尔曼增益,$\hat{\boldsymbol{x}}(k|k)$为当前时刻的后验状态估计值,$\boldsymbol{P}(k|k)$为当前时刻的后验状态误差协方差矩阵。

AFFKF算法与KF算法的区别在于式(11)中引入了自适应渐消因子$\eta(k)$,故式(11)可以改写为:

$$\boldsymbol{P}(k|k-1)=\eta(k)\boldsymbol{A}\boldsymbol{P}(k-1|k-1)\boldsymbol{A}^{\mathrm{T}}+\boldsymbol{Q}(k) \tag{15}$$

对于任意增益$\boldsymbol{K}(k)$,新息协方差可表示为:

$$\boldsymbol{\mu}_0(k)=\mathrm{E}\left[\boldsymbol{\varepsilon}(k)\boldsymbol{\varepsilon}(k)^{\mathrm{T}}\right]=\boldsymbol{H}\boldsymbol{P}(k|k-1)\boldsymbol{H}^{\mathrm{T}}+\boldsymbol{R}(k) \tag{16}$$

故新息自协方差可表示为:

$$\boldsymbol{\mu}_f(k)=\mathrm{E}[\boldsymbol{\varepsilon}(k+f)\boldsymbol{\varepsilon}(k)^{\mathrm{T}}] \tag{17}$$

式(17)中:$\boldsymbol{\varepsilon}(k+f)$表示第$k+f$时刻的新息向量,$f$为正整数;当使用最佳增益$\boldsymbol{K}(k)$时,不同时刻的新息向量之间不相关,即$\boldsymbol{\mu}_f(k)=0$,此时有以下等式成立:

$$\boldsymbol{P}(k|k-1)\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{K}(k)\hat{\boldsymbol{\mu}}_0(k)=0 \tag{18}$$

式(18)中:新息向量协方差估计$\hat{\boldsymbol{\mu}}_0(k)$基于渐消记忆指数得到,通过引入指数加权机制,对当前时刻的新息向量赋予更高权重,从而有效提升整体估计的精确度,计算方法如下所示:

$$\begin{cases}\hat{\boldsymbol{\mu}}_0(k)=d(k)\boldsymbol{\varepsilon}(k)\boldsymbol{\varepsilon}(k)^{\mathrm{T}}+(1-d(k))\hat{\boldsymbol{\mu}}_0(k-1)\\ d(k)=\dfrac{1-b}{1-b^k}\end{cases} \tag{19}$$

式(19)中:b为遗忘因子,一般取值在0.70~0.95之间。

结合式(10)、式(16)和式(19)可得到渐消因子$\eta(k)$的计算式:

$$\eta(k)=\max\left\{1,\frac{\mathrm{tr}(\boldsymbol{N}(k))}{\mathrm{tr}(\boldsymbol{M}(k))}\right\} \tag{20}$$

$$\boldsymbol{N}(k)=\hat{\boldsymbol{\mu}}_0(k)-\boldsymbol{H}\boldsymbol{Q}\boldsymbol{H}^{\mathrm{T}}-\boldsymbol{R}(k) \tag{21}$$

$$\boldsymbol{M}(k)=\boldsymbol{H}\boldsymbol{A}\boldsymbol{P}(k|k-1)\boldsymbol{A}^{\mathrm{T}}\boldsymbol{H}^{\mathrm{T}} \tag{22}$$

2.2 检测器设计

当系统受到攻击时,估计值$\hat{\boldsymbol{y}}(k|k)$与系统实际输出值$\tilde{\boldsymbol{y}}(k)$之间的残差出现显著的偏差;如果CPPS保持安全运行,则有$\hat{\boldsymbol{y}}(k|k)\approx\tilde{\boldsymbol{y}}(k)$。欧几里得距离通过计算估计值与实际输出值之间欧氏距离的大小来反映两者之间的相似程度,是常用的相似性检验方法之一,定义k时刻$\boldsymbol{r}(k)$的欧几里得距离为$\gamma(k)$:

$$\gamma(k)=\|\boldsymbol{r}(k)\|_2=\sqrt{\left(\sum_{i=1}^{n}(\tilde{\boldsymbol{y}}_i(k)-\hat{\boldsymbol{y}}_i(k|k))\right)} \tag{23}$$

则基于欧几里得距离的残差检验函数为:

$$\xi(\tilde{\boldsymbol{y}}(k),\hat{\boldsymbol{y}}(k|k))=\frac{\|\boldsymbol{r}(k)\|_2}{\|\tilde{\boldsymbol{y}}(k)\|_2\|\hat{\boldsymbol{y}}(k|k)\|_2} \tag{24}$$

基于无攻击时$\xi(\tilde{\boldsymbol{y}}(k),\hat{\boldsymbol{y}}(k|k))$的值设置阈值,并记为$\rho$,然后根据以下规则检测系统中是否存在攻击:

$$\begin{cases}\xi(\tilde{\boldsymbol{y}}(k),\hat{\boldsymbol{y}}(k|k))<\rho, & \text{不存在攻击}\\ \xi(\tilde{\boldsymbol{y}}(k),\hat{\boldsymbol{y}}(k|k))\geqslant\rho, & \text{存在攻击}\end{cases} \tag{25}$$

3 仿真算例

3.1 算例基本描述

本文将在3机6总线的电力系统中验证所提出的D-LAA攻击模型和攻击检测模型,对于所有负载总线l_i设置$P_{i,\mathrm{pu}}^{\mathrm{L}}=1$,假设CPPS中的最大负载功率是$P_{\mathrm{pu}}^{\mathrm{L,\,max}}=2$,同时发电机的标称转子角频率为60 Hz,离散系统的采样时间设置为$T=0.001$ s。电力系统中发电机的各项参数参考文献[12],电力系统和滤波器的初始值设置如下:

$$\boldsymbol{x}(0)=[-0.045;-0.058;-0.070;\ 0.000;\ 0.080;\ 0.010];$$

$$\boldsymbol{x}(0|0)=[-0.045;-0.058;-0.070;\ 0.000;\ 0.080;\ 0.010];$$

$$\boldsymbol{P}(0|0)=\begin{bmatrix}0.10&0.00&0.00&0.00&0.00&0.00\\0.00&0.15&0.00&0.00&0.00&0.00\\0.00&0.00&0.20&0.00&0.00&0.00\\0.00&0.00&0.00&0.40&0.00&0.00\\0.00&0.00&0.00&0.00&0.30&0.00\\0.00&0.00&0.00&0.00&0.00&0.50\end{bmatrix};$$

$$\hat{\mu}(0)=0;$$

$$\boldsymbol{Q}(0)=\begin{bmatrix}0.0058&0.0079&0.0091&0.0005&-0.0055&0.0022\\0.0079&0.0095&0.0108&-0.0002&-0.0080&0.0019\\0.0091&0.0108&0.0123&-0.0010&-0.0103&0.0017\\0.0005&-0.0002&-0.0010&0.0047&0.0087&0.0036\\-0.0055&-0.0080&-0.0103&0.0087&0.0220&0.0049\\0.0022&0.0019&0.0017&0.0036&0.0049&0.0032\end{bmatrix};$$

$$\boldsymbol{R}(0)=\begin{bmatrix}30&30&30&30&30&30\\30&30&30&30&30&30\\30&30&30&30&30&30\\30&30&30&30&30&30\\30&30&30&30&30&30\\30&30&30&30&30&30\end{bmatrix}。$$

系统正常运行时系统输出估计值$\hat{\boldsymbol{y}}(k|k)$与系统输出实际值$\tilde{\boldsymbol{y}}(k)$之间的残差函数值在0.002~0.016之间波动，故攻击检测阈值设置为$\rho=0.04$。

3.2　CPPS中的闭环D-LAA

从攻击者视角分析闭环D-LAA对CPPS稳定运行产生的影响，比较PI控制器和P控制器形式下闭环D-LAA的攻击效果。

假设l_4是CPPS中容易遭受攻击的脆弱负载，在第2 s向l_4注入闭环D-LAA，并考虑以窃电为目的和以发电机卸载为目的两种场景，系统转子角频率通过传感器总线$s=1$获得。

场景1：以窃电为目的

该场景中攻击参数$K_{\mathrm{P},41}^{\mathrm{L}}=5$，$K_{\mathrm{I},41}^{\mathrm{L}}=5$，$f_4^{\mathrm{L}}=0.2$。图2是D-LAA攻击下系统负载功率和发电机转子角频率偏差变化。

如图2(a)所示，D-LAA使系统内负载l_4的功率瞬间攀升至峰值，一段时间后负载功率波动逐渐减小并恢复稳定。攻击导致系统产生了额外的有功功率，存在窃电行为，造成了电网资源的浪费。图2(b)中D-LAA使发电机转子角频率出现较大的偏差，但得益于CPPS本身的保护机制和恢复能力，很快恢复了稳定。

P控制器和PI控制器下D-LAA造成的受害负载功率变化最大值和发电机转子角频率偏差最大值如表1所示。另外，从图2(a)中可以发现，当负载功率恢复稳定后，P控制器下D-LAA造成的受害负载功率明显小于PI控制器下D-LAA造成的

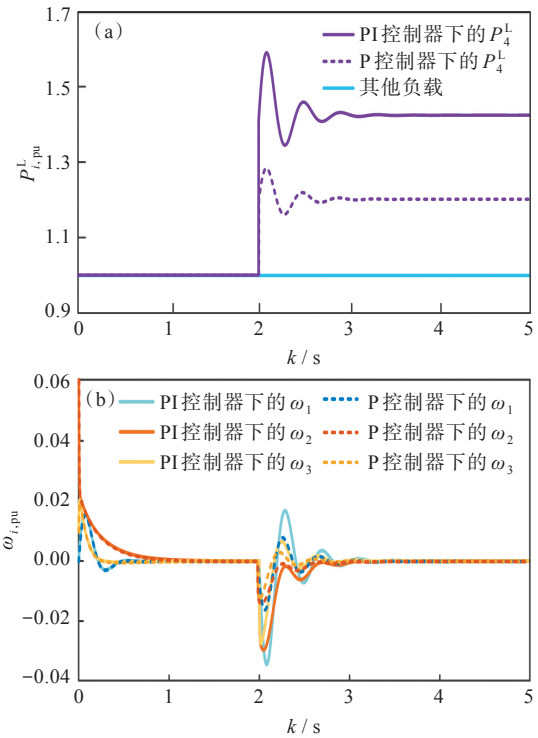

图2　以窃电为目的的D-LAA对CPPS的影响：(a)负载功率变化，(b)发电机转子角频率偏差变化

Fig. 2　Impact of electricity-theft-oriented D-LAA on the CPPS: (a) load power change, (b) generator rotor angular frequency deviation

受害负载功率。这是因为当CPPS受到P控制器下的D-LAA时，系统只受攻击产生的功耗的影响，而受到PI控制器下的D-LAA时，电网在恢复稳定后还会持续受之前攻击的影响。

表1　P控制器和PI控制器下的D-LAA参数对比

Table 1　Comparison of D-LAA parameters under P-controller and PI-controller

控制器类型	$P_{4,\mathrm{pu}}^{\mathrm{L,max}}$	$\omega_{1,\mathrm{pu}}^{\mathrm{max}}$	$\omega_{2,\mathrm{pu}}^{\mathrm{max}}$	$\omega_{3,\mathrm{pu}}^{\mathrm{max}}$
P控制器	1.282	0.928	0.769	0.404
PI控制器	1.599	2.064	1.742	0.910

场景2：以发电机卸载为目的

该场景中攻击参数$K_{\mathrm{P},41}^{\mathrm{L}}=10$，$K_{\mathrm{I},41}^{\mathrm{L}}=2$，$f_4^{\mathrm{L}}=0.1$。图3是D-LAA下系统的负载功率和发电机转子角频率偏差变化。

如图3(a)所示，以发电机卸载为目的的D-LAA使受攻击负载的功率逐渐增大至最大值，而场景1中受害负载的功率则在攻击瞬间突然增至最大。由图3(b)可知，以发电机卸载为目的的D-LAA使发电机的转子角频率偏差逐渐增大并达到其阈值。当D-LAA以P控制器的形式注入电网时，第1台发电机的转子角频率偏差在$t=4.584$ s时达到其阈值$\omega_{\mathrm{pu}}^{\mathrm{th}}=0.083$，从而导致发电机上的

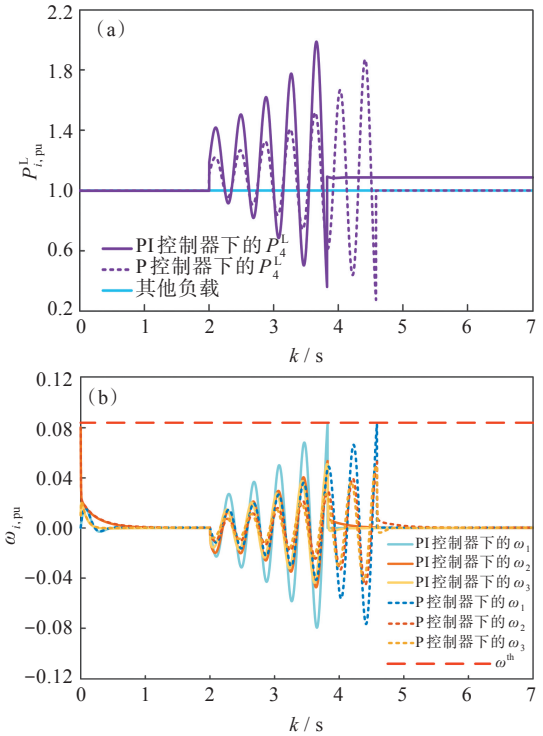

图3 以发电机卸载为目的的D-LAA对CPPS的影响：(a)负载功率变化，(b)发电机转子角频率偏差变化

Fig. 3 Impact of generation-unloading-oriented D-LAA on the CPPS: (a) load power change, (b) generator rotor angular frequency deviation

过频继电器跳闸，最终使总线1上的发电机卸载。然而，当D-LAA以PI控制器的形式注入电网时，时间被提前至3.821 s。由于攻击者以总线1上的发电机转子角频率作为反馈实施攻击，故总线1上的发电机被卸载后，攻击引起的受害负载功率和发电机转子角频率偏差波动立即消失。

由上述两个场景的仿真结果及分析可知，PI控制器下的D-LAA能造成更大的负载功率波动和发电机转子角频率偏差，且能在更短的时间内实现攻击。因此，后续主要对PI控制器下的D-LAA进行检测。

3.3 CPPS中的闭环D-LAA检测

从防御者视角，在上述两个场景中验证本文所提攻击检测方法的有效性。

场景1：以窃电为目的

图4(a)是发电机转子角频率偏差的测量值和在改进AFFKF下的估计值，可以看出改进AFFKF对大部分测量噪声进行了过滤。从图4(b)可以看出，攻击前发电机转子角频率偏差的估计值与真实值几乎相等，而当攻击发生后，估计值与真实值出现明显偏差。图4(c)是以窃电为目的的攻击检测结果，可以明显观察到在t = 2 s时攻击者向系统注入了攻击信号，t = 2.002 s时残差检测函数值突然上升并超过阈值，在t = 2.125 s时达到峰值，在t = 3 s后趋于稳定，且明显高于攻击发生前，这表明系统此时仍在受攻击的影响。此外，零时刻函数值出现大幅度上升是由于滤波器初始设置所引起，并不反映真实的攻击事件，通常被认为是正常现象。

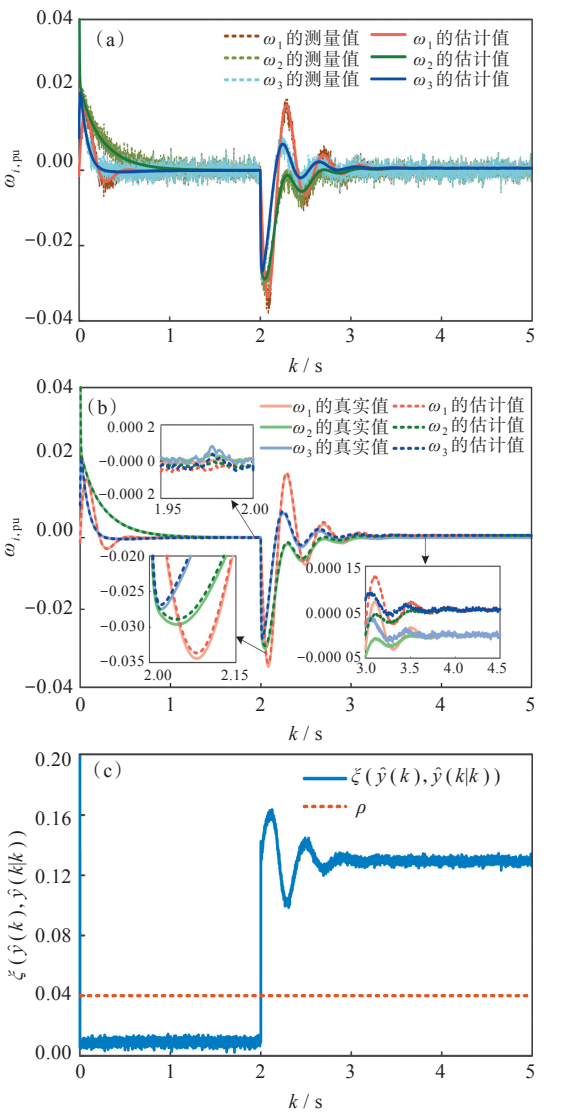

图4 以窃电为目的的D-LAA检测：(a)发电机转子角频率偏差测量值与估计值，(b)发电机转子角频率偏差真实值与估计值，(c)攻击检测结果

Fig. 4 Detection of electricity-theft-oriented D-LAA: (a) measured vs. estimated rotor angular frequency deviation of generators, (b) true vs. estimated rotor angular frequency deviation of generators, (c) attack detection result

场景2：以发电机卸载为目的

图5(a)–图5(c)分别是以发电机卸载为目的的D-LAA下ω_1、ω_2和ω_3的状态估计值，可以看出，与文献[18]中的算法相比，本文所提的改进AFFKF算法在系统被攻击时具有更高的估计精度。另外，在第1台发电机被卸载的瞬间，相较于

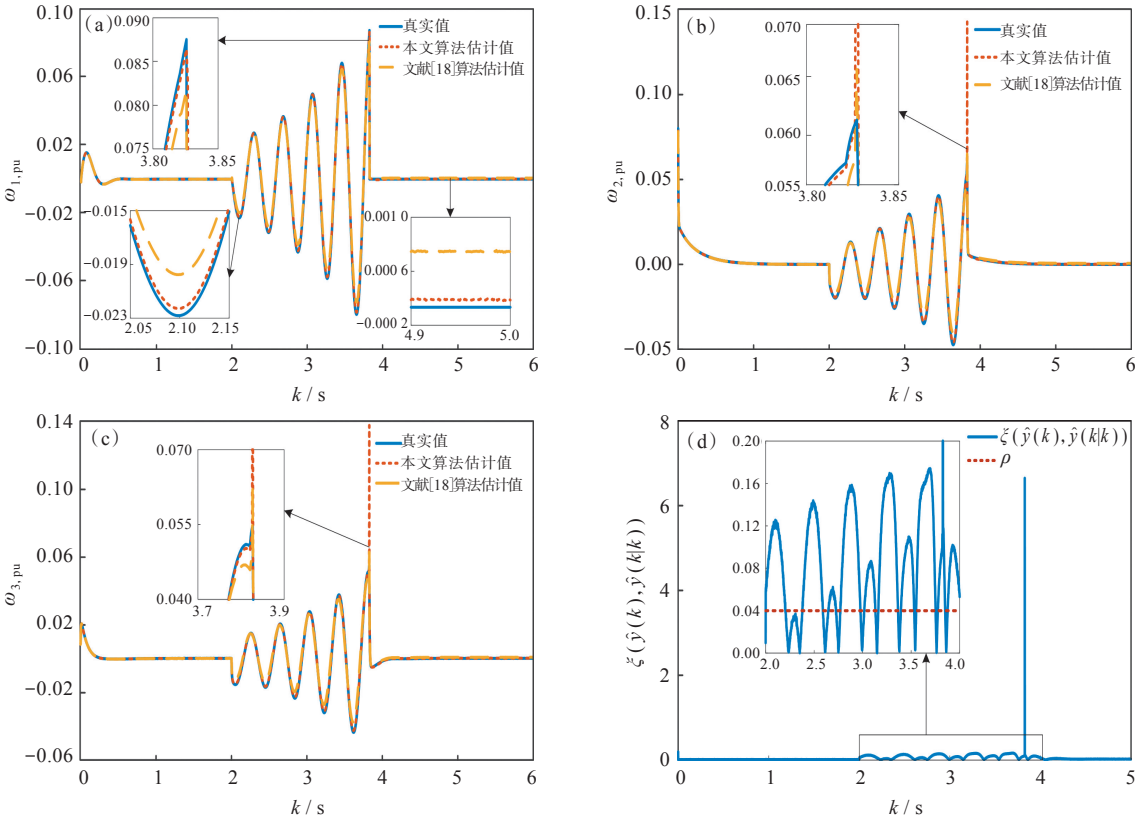

图5　以发电机卸载为目的的D-LAA检测：(a)ω_1的状态估计结果，(b)ω_2的状态估计结果，(c)ω_3的状态估计结果，(d)攻击检测结果

Fig. 5　Detection of generation-unloading-oriented D-LAA: (a) state estimation results ofω_1, (b) state estimation results of ω_2, (c) state estimation results of ω_3, (d) attack detection result

文献[18]中的算法，ω_2和ω_3在改进AFFKF算法下的状态估计值会明显增大，即对异常信号更加敏感。从图5(d)中可以看到在t = 2 s时残差函数开始出现波动并超过阈值，然后在t = 3.821 s时突然上升，随后立刻下降并趋于0，由此可知攻击者是利用了被卸载的发电机实施的攻击，即攻击者在第1台发电机的总线上安装了传感器。

4　结　论

本文围绕CPPS安全问题展开研究，提出基于PI控制器的D-LAA模型，使电网产生更大的功率波动和角频率偏移，在更短的时间内实现攻击；提出基于新息协方差估计值的AFFKF，其中新息协方差估计值由渐消记忆指数加权计算得到，显著提高了状态估计器的估计精度和面对信号突变时的敏感度；提出欧几里得距离和残差函数相结合的检验方法，不仅能及时检测到D-LAA，还能对攻击造成的影响进行持续监控。

参考文献

[1] 叶飞，钟晓静，关前锋. 电力信息物理系统的网络攻击建模、演化规律及应对成本研究[J]. 综合智慧能源，2024，46(5)：58-64.

[2] 王彪，刘洋，陈肖龙. 针对电力信息物理系统的网络攻击进展研究[C]//中国仿真学会. 第三十四届中国仿真大会暨第二十一届亚洲仿真会议论文集. 北京：中国仿真学会，2022：66-74.

[3] 李沁雪，刘永桂，黎善斌，等. 基于入侵检测的信息物理系统攻击识别综述[J]. 控制工程，2022，29(6)：1049-1057.

[4] 张超. 城市数字化转型背景下关键基础设施信息物理系统安全建设对策研究[J]. 上海管理科学，2022，44(1)：80-83.

[5] 胡中功，程思婷，沈斌，等. DDoS攻击检测模型的设计[J]. 武汉工程大学学报，2017，39(1)：91-95.

[6] 胡翔，熊余，张祖凡. DOS攻击下饱和脉冲多智能体系统的安全定制化一致性[J]. 自动化学报，2024，50(12)：2499-2512.

[7] 程伶俐，石榆，詹习生. 基于T-S模糊模型的信息物理系统中分布式FDI攻击检测[J]. 控制与决策，2025，40(8)：2429-2438.

[8] 李卓，谢耀滨，吴茜琼，等. 基于深度学习的电力系统虚假数据注入攻击检测综述[J]. 电力系统保护与控制，2024，52(19)：175-187.

[9] 席磊，王文卓，白芳岩，等. 基于最大信息系数-双层置信极端梯度提升树的电网虚假数据注入攻击定位

检测[J]. 电网技术,2025,49(2):824-833.
[10] SHEN Y H, QIN Z J. Detection, differentiation and localization of replay attack and false data injection attack based on random matrix[J]. Science Reports, 2024,14:2758.
[11] MOHSENIAN-RAD A H, LEON-GARCIA A. Distributed internet-based load altering attacks against smart power grids [J]. IEEE Transactions on Smart Grid,2011,2(4):667-674.
[12] AMINI S, MOHSENIAN-RAD H, PASQUALETTI F. Dynamic load altering attacks in smart grid[C]// 2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). Piscataway, NJ:IEEE,2015:7131791.
[13] AMINI S, PASQUALETTI F, MOHSENIAN-RAD H. Dynamic load altering attacks against power system stability: attack models and protection schemes [J]. IEEE Transactions on Smart Grid, 2018,9(4):2862-2872.
[14] KAZEMI Z, SAFAVI A A, AREFI M M, et al. Finite-time secure dynamic state estimation for cyber-physical systems under unknown inputs and sensor attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics:Systems,2022,52(8):4950-4959.
[15] 穆建君,周川,郭健,等. 基于自适应简化容积卡尔曼滤波的编队卫星相对导航[J]. 南京理工大学学报,2023,47(3):365-372.
[16] LIN C Y, KAU L J, CHAN C Y. Bimodal extended Kalman filter-based pedestrian trajectory prediction [J]. Sensors,2022,22:8231.
[17] 刘康安,张伟伟,肖永超,等. 基于自适应无迹卡尔曼滤波的四旋翼无人机姿态解算[J]. 电光与控制,2022,29(7):126-131.
[18] LI J, SUN C W, YANG S X, et al. Dynamic load altering attack detection based on adaptive fading Kalman filter in smart grid [J]. IET Generation, Transmission & Distribution,2024,18:303-313.
[19] LI J, WANG Y F, SU Q Y. Dynamic load altering attack detection in smart grid based on multiple fading factor adaptive Kalman filter [J]. Electric Power System Research,2023,225:109834.

本文编辑:霍淑利

☆

(上接第286页)

[20] MAHMOUD I, BOUDEN S, CHARFI R, et al. Prevalence and impact of antibodies against TNF alpha inhibitors in Rheumatoid arthritis and spondyloarthritis: systematic review and meta-analysis with subgroup analysis [J]. Current Drug Safety, 2026, 21(2):108-128.
[21] 颜春鲁, 石杨洋, 宋佳眙, 等. 藤黄健骨胶囊通过调控TNF-α/IL-6/JAK2/STAT3通路抑制肾虚血瘀型绝经后骨质疏松患者Th17细胞分化的机制研究[J]. 中国现代应用药学, 2025, 42(14): 2445-2452.
[22] 沈燚, 孙艺琦, 李鹤鸣, 等. 巴戟天环烯醚萜苷下调GSK-3β抑制JAK2/STAT3和NF-κB通路减轻Ⅱ型胶原诱导的关节炎大鼠骨破坏的机制[J]. 药学学报, 2024, 59(10): 2763-2772.
[23] FINCKH A, GILBERT B, HODKINSON B, et al. Global epidemiology of rheumatoid arthritis [J]. Nature Reviews Rheumatology,2022,18(10):591-602.
[24] MENG W R, LI L, HAO Y Y, et al. NAD+ metabolism reprogramming mediates irradiation-induced immunosuppressive polarization of macrophages [J]. International Journal of Radiation Oncology Biology Physics, 2025,121(1): 176-190.
[25] 马青, 刘建成, 李春波. 槲皮素通过ERK1/2信号通路对主动脉夹层小鼠血管平滑肌细胞转化的作用机制研究[J]. 中西医结合心脑血管病杂志, 2023, 21(13): 2400-2405.
[26] TANG M S, ZENG Y, PENG W J, et al. Pharmacological aspects of natural quercetin in rheumatoid arthritis [J]. Drug Design, Development and Therapy, 2022, 16: 2043-2053.
[27] HE X Y, WU T Y, HE H H, et al. Study of kaempferol in the treatment of rheumatoid arthritis through modulation of the NLRP3/CASP1/GSDMD axis and T-cell activation: based on network pharmacology, single-cell analysis, and experimental validation [J]. International Immunopharmacology, 2024, 143: 113357.
[28] 周媛. DRG神经元膜离子通道介导的柚皮素缓解慢性疼痛的作用及机制研究[D]. 长春: 吉林大学, 2025.
[29] SU X H, LI T, LIU Z Q, et al. Licochalcone A activates Keap1-Nrf2 signaling to suppress arthritis *via* phosphorylation of p62 at serine 349 [J]. Free Radical Biology and Medicine, 2018, 115: 471-483.

本文编辑:张 瑞