引用格式:常梦言,刘永慧.混合攻击下基于容积卡尔曼滤波的多区域互联电力系统的检测与防御[J].电力科学与技术学报,2024,39(4):11-19.
Citation: CHANG Mengyan,LIU Yonghui.Detection and defense of multi-area interconnected power system based on cubature Kalman filter under hybrid attacks[J]. Journal of Electric Power Science and Technology,2024,39(4):11-19.

混合攻击下基于容积卡尔曼滤波的多区域互联电力系统的检测与防御

常梦言[1],刘永慧[2]
(1.上海电机学院电气学院,上海 201306;2.上海第二工业大学智能制造与控制工程学院,上海 201209)

摘　要:以多区域互联电力系统为研究对象,对混合攻击下多区域互联电力系统的检测与防御进行研究。首先,建立多区域互联电力系统的数学模型,分析多区域互联电力系统遭受网络攻击的位置及其类型,建立虚假数据注入攻击和拒绝服务攻击模型,接着根据是否收到数据包诊断拒绝服务攻击,并用最新接收的数据对丢失的数据进行补偿,实现拒绝服务攻击的防御;然后,基于容积卡尔曼滤波算法检测虚假数据注入攻击,并采用指数平滑法对虚假数据注入攻击进行防御;最后,以两区域互联电力系统为例进行仿真实验。仿真结果表明:所设计的控制算法能有效克服混合攻击对系统造成的不良影响,实现电力系统功率平衡和频率稳定。

关　键　词:多区域互联电力系统;容积卡尔曼滤波;虚假数据注入攻击;拒绝服务攻击;状态估计
DOI:10.19781/j.issn.1673-9140.2024.04.002　**中图分类号**:TM712;TP273　**文章编号**:1673-9140(2024)04-0011-09

Detection and defense of multi-area interconnected power system based on cubature Kalman filter under hybrid attacks

CHANG Mengyan[1], LIU Yonghui[2]
(1.School of Electrical Engineering, Shanghai Dianji University, Shanghai 201306, China; 2.School of Intelligent Manufacturing and Control Engineering, Shanghai Polytechnic University, Shanghai 201209, China)

Abstract: This paper takes the multi-regional interconnected power system as the research object, and studies the detection and defense of multi-region interconnected power system under hybrid attack. Firstly, a mathematical model of multi-regional interconnected power system is established, the location and type of network attacks suffered by multi-regional interconnected power system are analyzed, and false data injection attacks and denial of service attack models are established. Secondly, diagnose denial of service attacks based on whether packets are received, and the recently received packet compensates for the lost packet, the defense of denial-of-service attack is realized. Then, based on the cubature Kalman filter algorithm, false data injection attacks are detected, and exponential smoothing is used to defend against false data injection attacks. Finally, taking the two-region interconnected power system as an example, the simulation experiment shows that the designed control algorithm can effectively overcome the adverse effects of hybrid attacks on the system, and realize the power balance and frequency stability of the power system.

Key words: multi-area interconnected power system; cubature Kalman filter; false data injection attack; denial of service attack; state estimation

随着电网互联程度的增加,电力系统的规模日益庞大,结构也愈加复杂。通过电力系统的频率可以判断电力系统是否稳定运行,负荷的任意波动或外部参数的干扰都有可能导致多区域互联电力系统频率的剧烈振荡。负荷频率控制(load frequency control, LFC)系统的控制中心利用接收到的频率

收稿日期:2023-03-20;**修回日期**:2023-06-07
基金项目:国家自然科学基金(61803253)
通信作者:刘永慧(1986—),女,博士,副教授,主要从事电力系统智能控制和切换系统研究;E-mail:liuyh@sspu.edu.cn

偏差与联络线功率计算出区域控制误差(area control error, ACE),将其作为控制发电机发出功率的控制信号,为维持电力系统频率稳定和功率平衡,调节调频发电机的出力可以使区域间按计划进行功率交换以及发电和负荷的实时平衡[1-2]。随着传统电力系统和信息通信网络深度融合,网络的开放性使系统可能遭受到网络攻击[3-4]。

LFC系统的控制决策过程依靠网络通信,其必然存在遭受网络攻击的潜在威胁。攻击者通过控制中心与远程终端之间的通信,破坏LFC协调电力系统运行的能力[5],如开展虚假数据注入(false data injection, FDI)攻击、拒绝服务(denial of service, DoS)攻击等,其中FDI攻击通过篡改LFC系统接收的频率和功率,使LFC系统超调引发频率波动,甚至使频率越界[1]。DoS攻击通过阻塞传输节点或阻塞传输信道,使信息的可用性遭到破坏,从而导致部分信息丢失,破坏系统的稳定性[6-7]。因此,研究LFC系统中网络攻击的检测与防御具有重要意义。

近年来,针对LFC系统中的网络攻击,学者们提出了一些不同的检测和控制方法。其中,LFC系统中FDI攻击的检测方法主要有基于ACE监测的预测方法和基于LFC系统状态观测方法2种[1]。第1种检测法主要采用机器学习算法,如多层感知分类器、人工神经网络来检测FDI攻击。文献[8-9]基于多层感知分类器的方法,通过对比正常运行和遭受攻击时的区域误差,区分受损信号与正常信号;为缓解FDI攻击对LFC系统造成的影响,文献[10-11]采用长短期记忆网络学习对ACE进行预测,通过对比预测值和ACE测量值检测FDI攻击。第1种检测法在对FDI攻击进行学习时,要收集被攻击系统足够多的数据,然而网络攻击下收集系统的真实数据无法实现,从而限制了其应用[12]。第2种检测法是对LFC系统进行状态估计,通过对比状态估计值和真实量测值检测FDI攻击。文献[13]提出了一种基于加权最小二乘观测器的FDI攻击检测方法;文献[14]基于卡尔曼滤波对LFC系统进行状态估计,并利用估计残差检测FDI攻击;文献[15]设计了未知输入观测器和卡尔曼滤波器,在模型不确定性的情况下提高了系统的性能。

针对LFC系统中DoS攻击的检测与防御已经取得一些研究成果。文献[16]基于元细胞计算网络预测量测数据替代丢包数据,抑制了DoS攻击的影响;为研究DoS攻击下多区域互联电力系统的安全控制问题,文献[17-18]提出了一种弹性事件触发机制,使多区域互联电力系统可以弥补DoS攻击所造成的不良影响;在此基础上,文献[19]进一步提出了自适应弹性事件触发控制,通过动态调整事件触发参数,节省了通信资源。值得注意的是,上述LFC系统中针对网络攻击的研究仅考虑了FDI攻击或DoS攻击,然而在实际系统中,LFC系统中的网络攻击可能发生在各种控制区域或传输通道中,恶意攻击者可以同时发动多种不同的攻击。与此同时,当遭受FDI攻击时,电力系统不仅需要检测FDI攻击,更要保证在不停机的情况下持续安全生产电能,因此,在混合攻击下设计有效的网络攻击检测与防御策略具有重要的意义。

针对LFC系统中检测混合攻击的基础上,如何防御混合攻击的问题,本文基于容积卡尔曼滤波(cubature Kalman filter, CKF)对系统中混合攻击的检测与防御进行研究。首先建立多区域互联电力系统的负荷频率控制数学模型;然后运用伯努利分布对DoS攻击进行建模,并使用最新接收的数据补偿丢失的数据,实现DoS攻击的防御;接着基于CKF算法利用估计残差检测FDI攻击,并采用指数平滑法预测的ACE替代由FDI攻击下计算得到的ACE,实现FDI攻击的防御;最后通过仿真实验验证所提算法的有效性。

1 建立系统模型

频率稳定和功率平衡是电力系统最基本的要求,在电力系统中,LFC负责将系统频率和区域之间的功率交换并保持在所需的计划值内[20]。多区域互联电力系统具有复杂非线性的特点,在负荷频率控制中,因正常运行时负荷的变化非常小,故可以将系统模型线性化处理。多区域互联电力系统第i区域的LFC框图如图1所示。

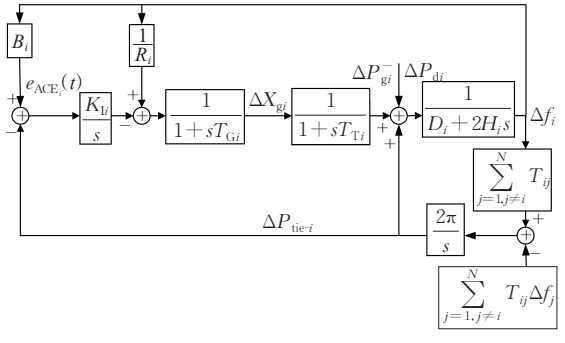


图1 多区域电力系统第i个区域的LFC框图

Figure 1 Block diagram of load frequency control for area i of multi-area power system

系统的数学模型为

$$\begin{cases}\Delta\dot{f}_i(t)=-\dfrac{D_i}{2H_i}\Delta f_i(t)+\dfrac{1}{2H_i}\Delta P_{gi}(t)-\\ \qquad\qquad\dfrac{1}{2H_i}u_i(t)-\dfrac{1}{2H_i}\Delta P_{\text{tie-}i}(t)\\ \Delta\dot{P}_{gi}(t)=-\dfrac{1}{T_{Ti}}\Delta P_{gi}(t)+\dfrac{1}{T_{Ti}}\Delta X_{gi}(t)\\ \Delta\dot{X}_{gi}(t)=-\dfrac{1}{R_iT_{Gi}}\Delta f_i(t)-\dfrac{1}{T_{Gi}}\left(\Delta X_{gi}(t)-e_{\text{ACE}_i}(t)\right)\\ \Delta\dot{P}_{\text{tie-}i}=2\pi\sum\limits_{j=1,i\neq1}^{N}T_{ij}\Delta f_i\\ \dot{e}_{\text{ACE}_i}(t)=-K_{Ii}B_i\Delta f_i(t)-K_{Ii}\Delta P_{\text{tie-}i}(t)\end{cases}\tag{1}$$

式中,$\Delta f_i(t)$为频率偏差;$\Delta P_{gi}(t)$为涡轮输出功率;$\Delta X_{gi}(t)$为调速器阀门位置偏差;$\Delta P_{\text{tie-}i}(t)$为联络线的功率交换;$e_{\text{ACE}_i}(t)$为区域控制偏差;$H_i$为惯性系数;$D_i$为频率灵敏度负载系数;$T_{Ti}$为涡轮时间常数;$R_i$为调速系数;$T_{Gi}$为调速器的时间常数;$B_i$为频率偏差因子,$B_i=1/R_i+D_i$;$T_{ij}$为区域$i$、$j$联络线同步系数;$K_{Ii}$为积分控制常数。

对式(1)进行化简,得到系统的状态方程为

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

式中,w为过程噪声;υ为量测噪声,$\boldsymbol{x}(t)=[\boldsymbol{x}_1(t)\ \boldsymbol{x}_2(t)\ \cdots\ \boldsymbol{x}_n(t)]^{\mathrm{T}}$为系统状态,其中$\boldsymbol{x}_i(t)=[\Delta f_i\ \ \Delta P_{gi}\ \ \Delta X_{gi}\ \ \Delta P_{\text{tie-}i}\ \ e_{\text{ACE}_i}]^{\mathrm{T}}$;$\boldsymbol{u}=[u_1,u_2]^{\mathrm{T}}$为系统输入;$\boldsymbol{z}(t)=[\boldsymbol{z}_1(t)\ \boldsymbol{z}_2(t)\ \cdots\ \boldsymbol{z}_n(t)]^{\mathrm{T}}$为系统量测量,其中$\boldsymbol{z}_i(t)=\left[\Delta f_i(t),\Delta P_{\text{tie-}i}(t)\right]^{\mathrm{T}}$。系统参数如下:

$$\boldsymbol{A}=\begin{bmatrix}\boldsymbol{A}_{11}&\boldsymbol{A}_{12}&\cdots&\boldsymbol{A}_{1N}\\ \boldsymbol{A}_{21}&\boldsymbol{A}_{22}&\cdots&\boldsymbol{A}_{2N}\\ \vdots&\vdots&\ddots&\vdots\\ \boldsymbol{A}_{N1}&\boldsymbol{A}_{N2}&\cdots&\boldsymbol{A}_{NN}\end{bmatrix}$$

$$\boldsymbol{A}_{ii}=\begin{bmatrix}-D_i/2H_i&1/2H_i&0&-1/2H_i&0\\ 0&-1/T_{Ti}&1/T_{Ti}&0&0\\ -1/R_iT_{Gi}&0&-1/T_{Gi}&0&1/T_{Gi}\\ 2\pi\sum\limits_{j=1,i\neq1}^{N}T_{ij}&0&0&0&0\\ -K_{Ii}B_i&0&0&-K_{Ii}&0\end{bmatrix}$$

$$\boldsymbol{A}_{ij}=\begin{bmatrix}0&0&0&0&0\\ 0&0&0&0&0\\ 0&0&0&0&0\\ -2\pi T_{ij}&0&0&0&0\\ 0&0&0&0&0\end{bmatrix}$$

$$\boldsymbol{B}=\mathrm{diag}\{\boldsymbol{B}_1,\boldsymbol{B}_2,\cdots,\boldsymbol{B}_N\}$$

$$\boldsymbol{B}_i=\left[-1/2H_i\quad0\quad0\quad0\quad0\right]^{\mathrm{T}}$$

$$\boldsymbol{C}=\mathrm{diag}\{\boldsymbol{C}_1,\boldsymbol{C}_2,\cdots,\boldsymbol{C}_N\}$$

$$\boldsymbol{C}_i=[1\quad0\quad0\quad1\quad0]^{\mathrm{T}}$$

2　网络攻击模型

在LFC系统中,频率量测和联络线功率量测为LFC系统的输入,ACE为LFC系统的输出控制发电机发出的功率。遭受网络攻击的LFC系统的系统框图如图2所示,可知攻击者会对频率传感器和联络线功率传感器实施FDI攻击,恶意篡改系统接收到的频率和功率数据$\boldsymbol{z}_i(t)=\left[\Delta f_i(t),\Delta P_{\text{tie-}i}(t)\right]^{\mathrm{T}}$;攻击者还会对频率量测和联络线功率量测的传输信道实施DoS攻击,使LFC系统无法收到频率和联络线功率数据,导致发电机收到错误的发电指令[21]。

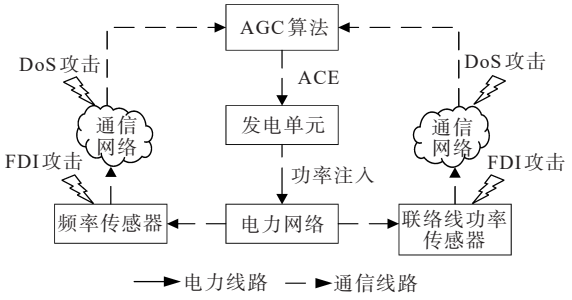


图2　存在潜在网络攻击的LFC系统框图

Figure 2　Block diagram of LFC system with potential cyber attacks

2.1　FDI攻击模型

FDI攻击通过篡改LFC系统接收的频率和功率数据,使LFC系统超调引发频率波动。本文考虑的FDI攻击模型为随机攻击,随机攻击将随机值$\mathrm{rank}(a,b)$添加到量测量z_k中,使得

$$z_k=\begin{cases}\boldsymbol{C}x_k+\upsilon_k, & k<\tau\\ \boldsymbol{C}x_k+\mathrm{rank}(a,b)+\upsilon_k, & k\geqslant\tau\end{cases}\tag{3}$$

式中,a、b分别为随机函数的下界和上界;τ为攻击者活跃的瞬间;υ_k为量测噪声。

2.2　DoS攻击模型

一定时间内DoS攻击为了使系统的通信受到干扰,其会阻塞传输信道或阻塞传输节点,造成量测量z_k丢包,满足:

$$z_k=\begin{cases}\boldsymbol{C}x_k+\upsilon_k, & k<\tau\\ \upsilon_k, & k\geqslant\tau\end{cases}\tag{4}$$

3 网络攻击的检测

当电力系统遭受网络攻击时，为了抵御网络攻击对系统造成的影响，需要先对网络攻击进行检测，并根据检测的结果对网络攻击进行防御。

3.1 检测DoS攻击

假设攻击者最多发起d次连续的DoS攻击，数据包在$k-d$时刻传输成功，攻击者在下一时刻发起攻击，则从$k-d$时刻到k时刻最多有d个数据包丢失。为了表示$z_k, z_{k-1}, \cdots, z_{k-d+1}, z_{k-d}$的传输状态，定义行矩阵$\boldsymbol{\lambda}_k$，其均服从伯努利分布特性[22]，满足：

$$\begin{cases} \Pr(\boldsymbol{\lambda}_k(i)=0)=\rho \\ \Pr(\boldsymbol{\lambda}_k(i)=1)=1-\rho \\ \mathrm{var}(\boldsymbol{\lambda}_k(i))=\rho(1-\rho) \end{cases} \tag{5}$$

式中，$\Pr(\cdot)$为概率；$\mathrm{var}(\cdot)$为方差；$\boldsymbol{\lambda}_k(i)$为$\boldsymbol{\lambda}_k$第$i$个元素，表示$z_{k-i+1}$的传输状态，$i\in[1, d+1]$，$\boldsymbol{\lambda}_k(i)=0$时表示量测数据受到DoS攻击，$\boldsymbol{\lambda}_k(i)=1$时表示量测数据未遭受DoS攻击。

k时刻z_k传输成功与否采用$\tilde{z}_k$表示，即

$$\tilde{z}_k=\boldsymbol{\lambda}_k(i)z_k,\ i=1 \tag{6}$$

式中，$\tilde{z}_k$为状态估计数据接收端收到的数据，$\tilde{z}_k=0$时，表示量测数据受到DoS攻击，$\tilde{z}_k\neq 0$时表示量测数据未受到DoS攻击；z_k为k时刻真实量测值。

3.2 检测FDI攻击

CKF的基本思想是采用高斯加权积分的三阶球面径向容积定律，通过逼近积分项实现不同方向上的概率性滤波[23]。CKF算法包括状态量预测和量测值更新2个基本过程[24]，具体步骤如下。

1）预测系统状态。

依据球面—径向规则对状态量估计值生成一组等权值容积点[25]。容积点x_{k-1}^i满足：

$$x_{k-1}^i=\hat{x}_{k-1}+\sqrt{\boldsymbol{P}_{k-1}}\,\boldsymbol{\xi}_i,\ i=1,2,\cdots,2n \tag{7}$$

式中，$\hat{x}_{k-1}$、$\boldsymbol{P}_{k-1}$分别为$k-1$时刻的状态估计值和估计误差协方差矩阵；x_{k-1}^i为生成的容积采样点，其与第i个采样点相应的权值w_i满足：

$$\begin{cases} w_i=1/2n \\ \boldsymbol{\xi}=\sqrt{n}\left\{\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}\begin{bmatrix}0\\1\\\vdots\\0\end{bmatrix}\cdots\begin{bmatrix}0\\0\\\vdots\\1\end{bmatrix}\begin{bmatrix}-1\\0\\\vdots\\0\end{bmatrix}\begin{bmatrix}0\\-1\\\vdots\\0\end{bmatrix}\cdots\begin{bmatrix}0\\0\\\vdots\\-1\end{bmatrix}\right\} \\ \boldsymbol{\xi}_i=\sqrt{n}\ [1]_i,\ i=1,2,\cdots,2n \end{cases} \tag{8}$$

其中，$[1]_i$表示容积点集的第i列。

通过状态方程对容积点进行变换，得到$\tilde{x}_{k|k-1}^i=f(x_{k-1}^i, u_{k-1})$，对$\tilde{x}_{k|k-1}^i$进行加权，得到预测量为

$$x_{k|k-1}=\frac{1}{2n}\sum_{i=1}^{2n}\tilde{x}_{k|k-1}^i \tag{9}$$

状态预测值的协方差矩阵可表示为

$$\boldsymbol{P}_{k|k-1}=\frac{1}{2n}\cdot \sum_{i=1}^{2n}(\tilde{x}_{k|k-1}^i-x_{k|k-1})(\tilde{x}_{k|k-1}^i-x_{k|k-1})^{\mathrm{T}}+\boldsymbol{Q} \tag{10}$$

式中，$\boldsymbol{Q}$为过程噪声协方差矩阵。

2）更新量测值。

首先，在状态预报值周围生成等权值的容积点$x_{k|k-1}^i=\sqrt{\boldsymbol{P}_{k|k-1}}\,\boldsymbol{\xi}_i+x_{k|k-1}$；然后，通过量测方程对容积点进行变换，得到量测预报值的容积点$z_{k|k-1}^i=h\left(x_{k|k-1}^i\right)$；最后，加权得到量测量预报值：

$$z_{k|k-1}=\frac{1}{2n}\sum_{i=1}^{2n}z_{k|k-1}^i \tag{11}$$

量测量预报值误差协方差矩阵为

$$\boldsymbol{P}_{k|k-1}^{zz}=\frac{1}{2n}\cdot \sum_{i=1}^{2n}(z_{k|k-1}^i-z_{k|k-1})(z_{k|k-1}^i-z_{k|k-1})^{\mathrm{T}}+\boldsymbol{R} \tag{12}$$

式中，$\boldsymbol{R}$为量测量误差协方差矩阵。

互协方差矩阵为

$$\boldsymbol{P}_{k|k-1}^{xz}=\frac{1}{2n}\cdot \sum_{i=1}^{2n}(x_{k|k-1}^i-x_{k|k-1})(z_{k|k-1}^i-z_{k|k-1})^{\mathrm{T}} \tag{13}$$

由式(13)、(14)得到卡尔曼滤波增益为$\boldsymbol{K}_k=\boldsymbol{P}_{k|k-1}^{xz}\boldsymbol{P}_{k|k-1}^{zz})^{-1}$，结合实际值$z_k$和预测值$z_{k|k-1}$，对状态预测值进行后验校正，得到当前状态估计值$\tilde{x}_k=x_{k|k-1}+\boldsymbol{K}_k(z_k-z_{k|k-1})$，因此协方差矩阵更新为

$$\boldsymbol{P}_k=\boldsymbol{P}_{k|k-1}-\boldsymbol{K}_k\boldsymbol{P}_{k|k-1}^{zz}\boldsymbol{K}_k^{\mathrm{T}} \tag{14}$$

k时刻的量测量残差$\boldsymbol{e}_k=z_k z_{k|k-1}$；为检测FDI攻击，定义误差向量$\boldsymbol{g}_k=\boldsymbol{e}_k\times\mathrm{cov}\times\boldsymbol{e}_k^{\mathrm{T}}$，其中cov为$\boldsymbol{e}_k$的协方差矩阵。检测器将$\boldsymbol{g}_k$与预设的阈值进行比较，在没有攻击的情况下，该阈值选择为大于残差的最大范数。

4 网络攻击的防御

在检测网络攻击的基础上，设计简单有效的补偿措施会减小网络攻击对系统的不良影响。

4.1 防御DoS攻击

假设攻击者在k时刻对量测数据进行DoS攻击，且k时刻连续丢包的数量为β，为了补偿DoS攻

击下丢失的数据包,用k时刻之前最新接收到的数据包补偿DoS攻击下丢失的数据包。定义补偿矩阵$\boldsymbol{M}_k\in\mathbf{R}^{1\times(d+1)}$,补偿矩阵只有第$\delta$个元素的值为1,其余元素的值为0,且$\delta=\beta+1$。

假设$\lambda_k=[0\ 1\ 1\ 0\ 1\ 1]$,表示$z_k$、$z_{k-3}$数据包丢失,连续丢包数$\beta=1$,$\delta=\beta+1=2$,则补偿矩阵$\boldsymbol{M}_k=[0\ 1\ 0\ 0\ 0\ 0]$,即采用$z_{k-2}$补偿丢失的$z_k$。由于数据采集过程中$\lambda_k$可以看作是一个滑窗,$z_{k-3}$在$k-3$时刻已经被$z_{k-4}$补偿。

当攻击者最多发起的连续攻击数$d=2$时,假设$\lambda_k=[0\ 0\ 1\ 1\ 1\ 1]$,表示$z_k$、$z_{k-1}$数据包丢失,连续丢包数$\beta=2$,$\delta=\beta+1=3$,则补偿矩阵$\boldsymbol{M}_k=[0\ 0\ 1\ 0\ 0\ 0]$,即采用$z_{k-2}$补偿丢失的$z_k$,$z_{k-1}$在$k-1$时刻已经被$z_{k-2}$补偿。

由以上分析可知,当k时刻发生DoS攻击时,补偿后的量测数据为

$$\tilde{\boldsymbol{z}}_k=\boldsymbol{M}_k[z_k\ \ z_{k-1}\ \ \cdots\ \ z_{k-d}]^{\mathrm{T}}=\boldsymbol{z}_{k-\delta+1}\tag{15}$$

4.2　防御FDI攻击

指数平滑法是对过去观测值加权平均进行预测,将t时刻的实际值与t时刻预测值加权平均得到$t+1$时刻的预测值[26]。本文采用三次指数平滑法对ACE进行预测,采用三次指数平滑预测值更新遭受FDI攻击的量测值,计算得到ACE,实现FDI攻击的防御。

首先,将k时刻之前T个时刻的量测值$e_{\mathrm{ACE}}(k-T)$,$e_{\mathrm{ACE}}(k-T+1)$,…,$e_{\mathrm{ACE}}(k-1)$作为观测值输入指数平滑法;然后,确定平滑系数α,$\alpha\in[0,1]$,三次指数平滑法的计算公式[25]为

$$\begin{cases}S_{1(k)}=\alpha\tilde{x}_k+(1-\alpha)S_{1(k-1)}\\S_{2(k)}=\alpha\tilde{x}_{1(k)}+(1-\alpha)S_{2(k-1)}\\S_{3(k)}=\alpha\tilde{x}_{2(k)}+(1-\alpha)S_{3(k-1)}\end{cases}\tag{16}$$

利用$k-1$时刻的三次指数平滑值计算线性平滑参数c_{k-1}、b_{k-1}、c_{k-1},进而得到k时刻的ACE指数平滑预测值$e'_{\mathrm{ACE},k}$,即

$$\begin{cases}a_{k-1}=3S_{1(k-1)}-3S_{2(k-1)}+S_{3(k-1)}\\b_{k-1}=\dfrac{\alpha}{2(1-\alpha)^2}[(6-5\alpha)S_{1(k-1)}-(10-8\alpha)\cdot\\\qquad S_{2(k-1)}+(4-3\alpha)S_{3(k-1)}]\\c_{k-1}=\dfrac{\alpha^2}{2(1-\alpha)^2}(S_{1(k-1)}-2S_{2(k-1)}+S_{3(k-1)})\\e'_{\mathrm{ACE},k}=a_{k-1}+b_{k-1}+c_{k-1}\end{cases}\tag{17}$$

当检测到量测量中存在FDI攻击时,采用三次指数平滑预测值更新由不良数据进行计算的ACE,可减弱FDI攻击对电力系统功率平衡和频率稳定的影响。

根据对网络攻击的检测与防御的研究,混合攻击下基于CKF的多区域电力系统的检测与防御流程如图3所示。首先,根据状态估计接收端是否收到数据包判断是否发生DoS攻击;然后,基于伯努利分布分析DoS攻击的量测数据丢失特点,并且将最近一次接收到的数据包补偿丢失的数据包,实现DoS攻击的防御;最后,基于CKF算法检测FDI攻击,并采用指数平滑法预测ACE替代由FDI攻击下计算得到的ACE,实现FDI攻击的防御。

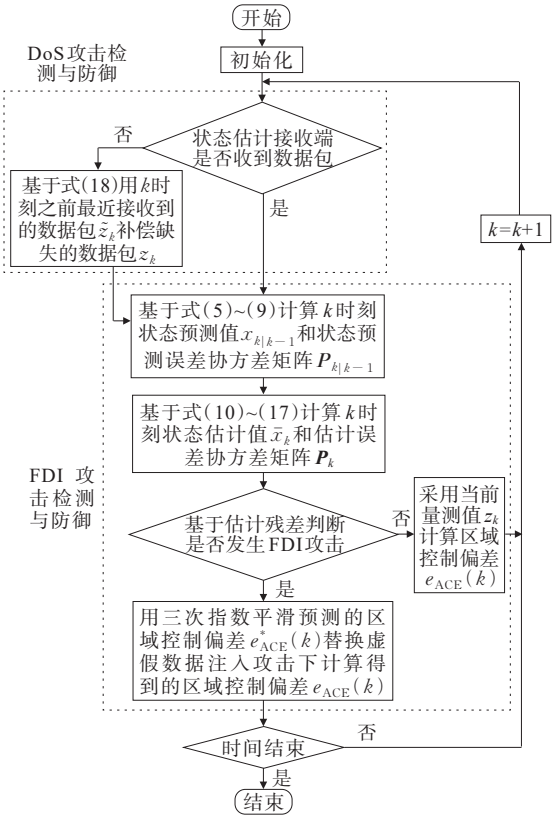


图3　混合攻击下基于CKF的多区域电力系统的检测与防御流程

Figure 3　Detection and defense flow of multi-area power system based on CKF under hybrid attack

5　仿真结果及分析

本文以FDI攻击和DoS攻击下的两区域互联电力系统为例,验证所提出的FDI攻击与DoS攻击检测与防御方法的有效性。CKF中过程噪声协方差满足高斯分布,设为$10^{-5}\boldsymbol{I}_1$,其中$\boldsymbol{I}_1$为10×10阶的单位矩阵,测量噪声协方差也满足高斯分布,设为$10^{-4}\boldsymbol{I}_2$,其中$\boldsymbol{I}_2$为4×4阶单位矩阵。考虑系统在$t\geqslant0$时遭受负载扰动,其值分别为$\Delta P_{\mathrm{d1}}=0.14$、$\Delta P_{\mathrm{d2}}=0.68$,系统参数如表1所示。

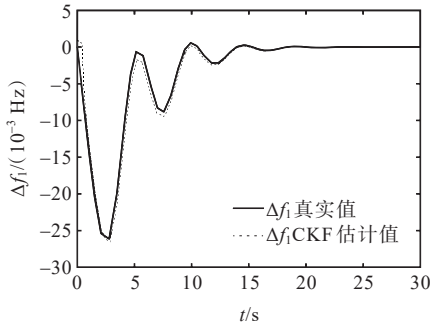
表1 区域系统参数

Table 1 Parameters of regional system

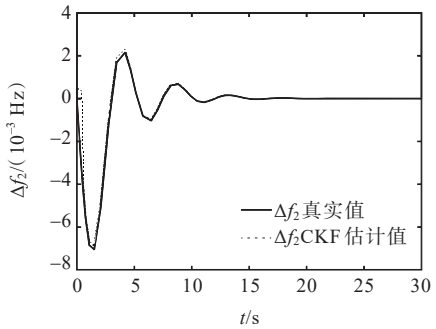
参数	区域1	区域2	参数	区域1	区域2
H_i	5.0	4.0	B_i	15.6	10.9
D_i	0.6	0.9	$1/R_i$	15.0	10.0
T_{Ti}	0.5	0.6	K_{Ii}	−0.3	−0.3
T_{Gi}	0.2	0.3			

5.1 CKF状态估计

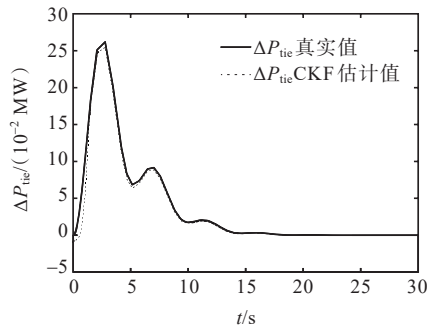
检测FDI攻击时采用CKF算法对系统进行状态估计，并根据估计的结果检测FDI攻击，因此，CKF算法估计系统状态的准确性会影响到后续FDI攻击的检测。无攻击时系统的CKF估计值与真实值对比如图4所示，可知CKF算法可以实现对多区域互联电力系统状态的准确估计。



(a) 系统频率偏差 $\Delta f_1(t)$



(b) 系统频率偏差 $\Delta f_2(t)$



(c) 联络线的功率 $\Delta P_{tie}(t)$

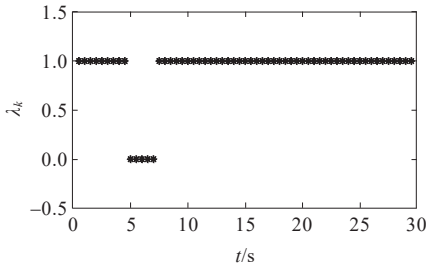
图4 无攻击时系统的CKF估计值与真实值对比

Figure 4 Comparison between CKF estimation results of system under no-attack conditions and true values

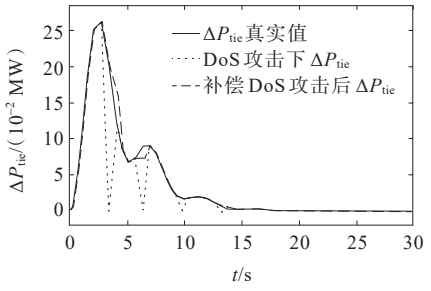
5.2 DoS、FDI以及混合攻击的检测与防御

1) DoS攻击的检测与防御。

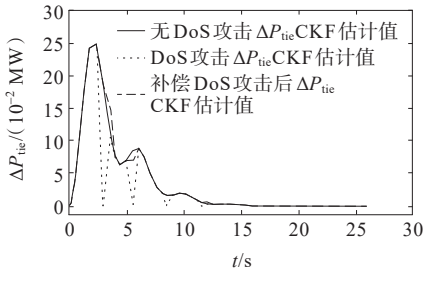
DoS攻击的检测与防御结果如图5所示，将式(4)的DoS攻击加入联络线功率量测中，假设量测数据丢失的概率为0.06，相对应的数据包丢失时序如图5(a)所示，其中“0”表示数据包丢失，“1”表示数据包传输正常。由图5(b)可以看出，在发生DoS攻击时，本文提出的DoS攻击防御方法可以有效抑制DoS攻击对联络线功率的影响。为验证该DoS攻击防御方法不会对后续FDI攻击的检测与防御阶段造成影响，分别将未加DoS攻击的量测数据、DoS攻击后的量测数据、防御DoS攻击后的量测数据输入CKF进行状态估计，由图5(c)可见，本文提出的DoS攻击防御方法对后续FDI攻击的检测与防御阶段造成影响较小。



(a) DoS攻击时序



(b) DoS攻击的防御



(c) 防御DoS攻击后CKF估计值

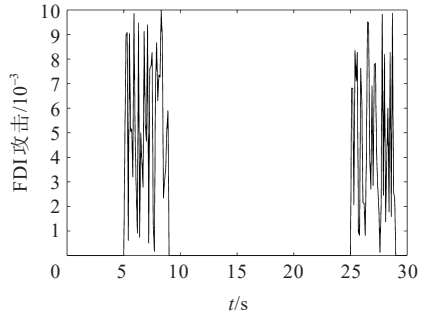
图5 DoS攻击的检测与防御

Figure 5 Detection and defense results of DoS attacks

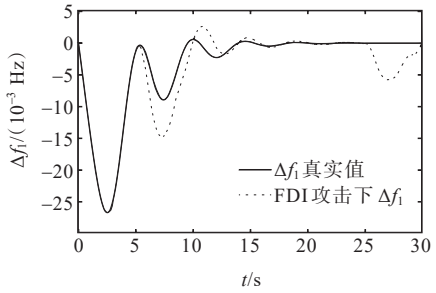
2)FDI攻击的检测与防御。

假设在第5、25 s时将式(3)的随机攻击加入区

域 1 频率偏差 $\Delta f_1(t)$,其上限为 0.01,下限为 0.00,攻击时长为 4 s。FDI 攻击下 $\Delta f_1(t)$ 如图 6 所示,可以看出,所加的 FDI 攻击会对区域 1 的频率稳定造成影响。



(a) FDI攻击



(b) FDI攻击前、后 $\Delta f_1(t)$ 对比

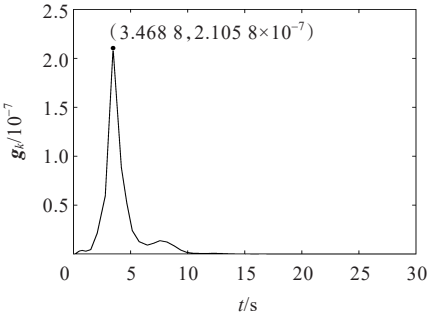
图 6　FDI 攻击下 $\Delta f_1(t)$

Figure 6　$\Delta f_1(t)$ under FDI attack

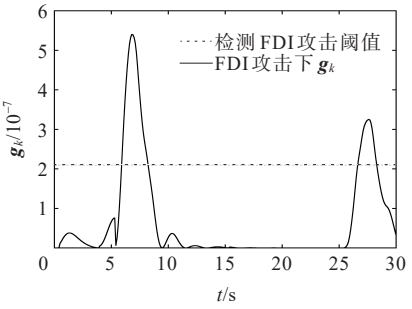
FDI 攻击的检测与防御结果如图 7 所示,由图 7(a)可以看出,未加 FDI 攻击时误差向量 $\boldsymbol{g}_k$ 的最大值为 $2.105\,8\times10^{-7}$,选取该最大值作为检测 FDI 攻击的阈值,将加入 FDI 攻击后计算的误差向量 $\boldsymbol{g}_k$ 与所选的阈值进行比较,由图 7(b)可以看出,此检测方法可以检测图 6(a)所示的 FDI 攻击。为了避免 FDI 攻击对 $\Delta f_1(t)$ 造成图 6(b)所示的影响,当检测到 FDI 攻击时,采用三次指数平滑法预测的 ACE 来更新由不良数据计算得到的 ACE,由图 7(c)可以验证所提 FDI 攻击防御方法的有效性。

3)混合攻击的检测与防御。

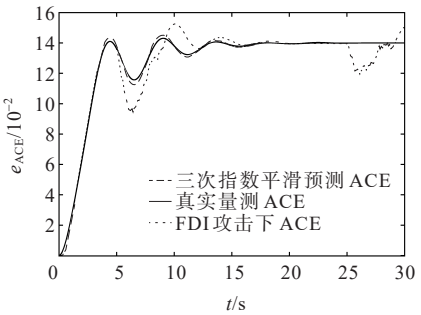
假设在第 5 s 将式(3)的随机攻击加入联络线功率 $\Delta P_{\text{tie-1}}(t)$,其上限为 0.01,下限为 0.00,攻击时长为 2 s;与此同时,将式(4)的 DoS 攻击加入联络线功率量测中。当同时发生 DoS 和 FDI 攻击时,由于 DoS 攻击会引起量测数据丢包,从而导致 FDI 攻击后的不良数据无法成功传输,因此,当 DoS 和 FDI 攻击同时发生时,采用针对 DoS 攻击的防御策略。混合攻击的防御结果如图 8 所示,可以看出,在同时发生 DoS 和 FDI 攻击时,本文提出的混合攻击防御方法可以有效抑制混合攻击对联络线功率的影响。



(a) 未加 FDI 攻击时误差向量 $\boldsymbol{g}_k$



(b) FDI 攻击的检测



(c) FDI 攻击的防御

图 7　FDI 攻击的检测与防御

Figure 7　Detection and defense results of FDI attacks

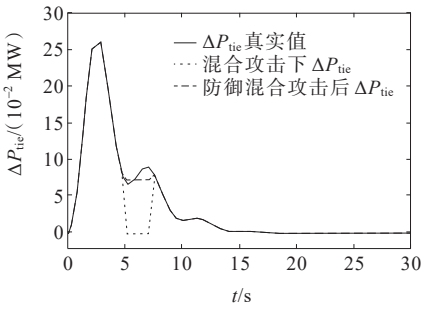


图 8　混合攻击的防御

Figure 8　Defense results against hybrid attacks

6 结语

本文对含有FDI攻击和DoS攻击的多区域电力系统负荷频率控制进行了研究。通过设计数据补偿策略实现DoS攻击的防御,采用CKF对系统进行状态估计,基于估计残差实现FDI攻击的检测,进一步采用三次指数平滑预测值更新由不良数据进行计算的ACE,实现FDI攻击的防御。结果表明:所提方法可以有效克服FDI和DoS攻击带来的不良影响。

参考文献:

[1] 徐飞阳,薛安成,常乃超,等.电力系统自动发电控制网络攻击与防御研究现状与展望[J].电力系统自动化,2021,45(3):3-14.
XU Feiyang, XUE Ancheng, CHANG Naichao, et al. Research status and prospect of cyber attack and defense on automatic generation control in power system[J]. Automation of Electric Power Systems,2021,45(3):3-14.

[2] 姚琦,胡阳,柳玉,等.考虑载荷抑制的风电场分布式自动发电控制[J].电工技术学报,2022,37(3):697-706.
YAO Qi, HU Yang, LIU Yu, et al. Distributed automatic generation control of wind farm considering load suppression[J]. Transactions of China Electrotechnical Society,2022,37(3):697-706.

[3] 唐云泽,苏晓茜.电力系统网络攻击方法研究综述[J].中国信息化,2020(12):57-60.
TANG Yunze, SU Xiaoqian. Survey of network attack methods of power system[J]. Information Technology in China,2020(12):57-60.

[4] 张亚健,彭晨,许东,等.蓄意流量攻击下基于确定网络演算的互联电网自适应负荷频率控制策略[J].电力系统保护与控制,2023,51(13):70-81.
ZHANG Yajian, PENG Chen, XU Dong, et al. Deterministic networked calculus-based adaptive load frequency control in interconnected power systems considering malicious traffic attacks[J]. Power System Protection and Control,2023,51(13):70-81.

[5] 吴英俊,汝英涛,刘锦涛,等.基于集员滤波的自动发电控制系统虚假数据注入攻击检测[J].电力系统自动化,2022,46(1):33-41.
WU Yingjun, RU Yingtao, LIU Jintao, et al. False data injection attack detection for automatic generation control system based on set-membership filtering[J]. Automation of Electric Power Systems, 2022, 46(1): 33-41.

[6] LIU J, GU Y, ZHA L, et al. Event-Triggered load frequency control for multiarea power systems under hybrid cyber attacks[J]. IEEE Transactions on Systems, 2019,49(8):1665-1678.

[7] 李欣,易柳含,刘晨凯,等.基于数据驱动的电力系统虚假数据注入攻击检测[J].智慧电力,2023,51 (2):30-37.
LI Xin,YI Liuhan,LIU Chenkai,et al.False data injection attacks detection in power system based on data-driven algorithm[J] Smart Power,2023,51 (2):30-37.

[8] CHEN C, ZHANG K, YUAN K, et al, Novel detection scheme design considering cyber attacks on load frequency control[J]. IEEE Transactions on Industrial Informatics,2018,14(5):1932-1941.

[9] 夏云舒,王勇,周林,等.基于改进生成对抗网络的虚假数据注入攻击检测方法[J].电力建设,2022,43 (3):58-65.
XIA Yunshu, WANG Yong, ZHOU Lin, et al. False Data injection attack detection method based on improved generative adversarial network[J] Electric Power Construction,2022,43 (3):58-65.

[10] KHALAF M, YOUSSEF A, EL-SAADANY E. Joint detection and mitigation of false data injection attacks in AGC systems[J].IEEE Transactions on Smart Grid,2019, 10(5):4985-4995.

[11] 刘威,邓巍.基于RBF神经网络的主动配电网通信过程安全态势感知方法[J].电网与清洁能源,2024,40 (5):52-58.
LIU Wei, DENG Wei. A security situation awareness method of active distribution network communication process based on RBF neural network[J]. Power System and Clean Energy,2024,40 (5):52-58.

[12] CHEN X,HU S,LI Y,et al.Co-estimation of state and FDI attacks and attack compensation control for multi-area load frequency control systems under FDI and DoS attacks[J].IEEE Transactions on Smart Grid,2022,13(3): 2357-2368.

[13] DENG R, XIAO G, LU R. Defending against false data injection attacks on power system state estimation[J]. IEEE Transactions on Industrial Informatics,2017,13(1): 198-207.

[14] JEVTIC A,ZHANG F,LI Q,et al.Physics- and learning-based detection and localization of false data injections in automatic generation control[J]. IFAC PapersOnLine, 2018,51(28):702-707.

[15] AMELI A,HOOSHYAR A,YAZDAVAR A H,et al.Attack detection for load frequency control systems using stochastic unknown input estimators[J]. IEEE Transactions on Information Forensics and Security, 2018,13(10):2575-2590.

[16] ZHONG X, JAYAWARDENE I, VENAYAGAMOORTHY G K,et al.Denial of service attack on tie-line bias control in a power system with PV plant[J]. IEEE Transactions on Emerging Topics in Computational Intelligence,2017,

1(5):375-390.

[17] 杨飞生,汪璟,潘泉,等.网络攻击下信息物理融合电力系统的弹性事件触发控制[J].自动化学报,2019,45(1):110-119.
YANG Feisheng, WANG Jing, PAN Quan, et al. Elastic event trigger control of cyber-physical converged power system under network attack[J]. Acta Automatica Sinica, 2019,45(1):110-119.

[18] 任志航.面向电力客户侧终端网络的高效入侵检测模型研究[J].电测与仪表,2022,59 (5):149-157.
REN Zhihang. Research on an efficient intrusion detection model for power client side terminal network [J]. Electrical Measurement & Instrumentation, 2022, 59 (5):149-157.

[19] LU K,ZENG G,LUO X,et al.An adaptive resilient load frequency controller for smart grids with DoS attacks[J]. IEEE Transactions on Vehicular Technology,2020,69(5):4689-4699.

[20] 王政豪,刘永慧,韩美杰.基于自适应滑模的多区域时滞电力系统负荷频率控制[J].东华大学学报(自然科学版),2021,47(3):129-134.
WANG Zhenghao, LIU Yonghui, HAN Meijie. Load frequency control of multi-area time-delay power system based on adaptive sliding mode[J]. Journal of Donghua University(Natural Science),2021,47(3):129-134.

[21] CHEN C, CHEN Y, ZHAO J, et al. Data-driven resilient automatic generation control against false data injection attacks[J]. IEEE Transactions on Industrial Informatics, 2021,17(12):8092-8101.

[22] 李雪,李雯婷,杜大军,等.拒绝服务攻击下基于UKF的智能电网动态状态估计研究[J].自动化学报,2019,45(1):120-131.
LI Xue,LI Wenting,DU Dajun,et al.Research on dynamic state estimation of smart grid based on UKF under denial-of-service attack[J].Acta Automatica Sinica,2019, 45(1):120-131.

[23] 张叶贵,刘敏.基于容积卡尔曼滤波的配电网状态估计[J].电力科学与工程,2019,35(11):26-30.
ZHANG Yegui,LIU Min,State estimation of distribution network based on cubature Kalman filter[J]. Electric Power Science and Engineering,2019,35(11):26-30.

[24] 王彤,高明阳,黄世楼,等.基于自适应容积卡尔曼滤波的双馈风力发电机动态状态估计[J].电网技术,2021,45(5):1837-1845.
WANG Tong, GAO Mingyang, HUANG Shilou, et al. Dynamic state estimation of doubly-fed wind turbines based on adaptive volumetric Kalman filtering[J]. Power System Technology,2021,45(5):1837-1845.

[25] 朱茂林,刘灏,毕天姝,等.考虑输入量不良数据的发电机动态状态估计方法[J].电力系统自动化,2022,46(7):94-103.
ZHU Maolin, LIU Hao, BI Tianshu, et al. Dynamic state estimation method for generators considering bad data in input[J]. Automation of Electric Power Systems,2022,46 (7):94-103.

[26] 王国权,王森,刘华勇,等.基于自适应的动态三次指数平滑法的风电场风速预测[J].电力系统保护与控制,2014,42(15):117-122.
WANG Guoquan, WANG Sen, LIU Huayong, et al. Wind speed prediction of wind farm based on adaptive dynamic cubic exponential smoothing method[J]. Power System Protection and Control,2014,42(15):117-122.