控制与决策
Control and Decision

FDI攻击下互联电力系统的分布式安全状态估计

翁世清, 翁品迪, 周京, 陈博, 苏子漪

引用本文:
翁世清,翁品迪,周京,陈博,苏子漪. FDI攻击下互联电力系统的分布式安全状态估计[J]. 控制与决策, 2023, 38(7): 1935−1941.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2021.1535

FDI攻击下互联电力系统的分布式安全状态估计

翁世清[1], 翁品迪[1], 周 京[1], 陈 博[1†], 苏子漪[2]

(1. 浙江工业大学 信息工程学院，杭州 310023； 2. 浙江树人大学 信息科技学院，杭州 310023)

摘 要: 针对虚假数据注入(FDI)攻击下的多区域互联电力系统安全状态估计问题,提出一种分布式中间观测器,同时对各区域电力系统的状态、虚假数据注入攻击信号以及负载偏差进行估计. 首先,通过将电力系统的状态和虚假数据注入攻击进行增广,得到等价的区域电力系统状态空间模型;然后,基于等价系统模型构建分布式中间观测器,对各个电力子系统分别进行安全状态估计,并设计补偿控制策略以降低虚假数据注入攻击及负载偏差带来的影响;最后,通过算例仿真验证所提出方法的可行性和有效性.

关键词: FDI攻击；多区域互联电力系统；安全估计；分布式中间观测器；负载偏差；补偿控制

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2021.1535 **开放科学(资源服务)标识码(OSID):**

引用格式: 翁世清,翁品迪,周京,等. FDI攻击下互联电力系统的分布式安全状态估计[J]. 控制与决策, 2023, 38(7): 1935-1941.

Distributed secure state estimation for interconnected power systems under FDI attacks

WENG Shi-qing[1], *WENG Pin-di*[1], *ZHOU Jing*[1], *CHEN Bo*[1†], *SU Zi-yi*[2]

(1. College of Information Engineering，Zhejiang University of Technology，Hangzhou 310023，China；2. College of Information Science and Technology，Zhejiang Shuren University，Hangzhou 310023，China)

Abstract: This paper focuses on the problem of multi-area interconnected power system secure state estimation under false data injection (FDI) attack. A distributed intermediate observer method is proposed to estimate the system states, FDI attack signals and load deviation of the system simultaneously. Firstly, the states of a power system and the FDI attack are augmented to obtain the equivalent state space model. Then, a distributed intermediate observer is constructed for each power subsystem to fulfill secure estimation, and a compensation control strategy is designed to reduce the impact of FDI attack and load deviation. Finally, the simulation results show that the proposed method is feasible and effective.

Keywords: FDI attack; multi-area interconnected power systems; security estimation; distributed intermediate observer; load deviation; compensating control

0 引 言

电力设施作为社会重要的基础设施之一,其安全运行对国家的各个领域都有着重大意义. 近年来,随着信息化技术的发展以及碳达峰、碳中和目标的提出,构建新型电力信息物理系统,发展数字能源以及数字电网势在必行. 然而,新型电力系统与通信系统、监控系统的深度融合[1],在满足数字化电网“可见、可知、可控”需求的同时,也提高了恶意网络攻击对系统安全运行的威胁[2]. 常见的网络攻击包括拒绝服务攻击[3]、时延攻击[4]以及虚假数据注入(false data injection, FDI)攻击[5]等,其中FDI攻击能够恶意篡改系统数据,具有隐蔽性高、破坏性强的特点[6-7],一旦成功入侵,将会影响电力系统的稳定运行,甚至造成供电故障. 因此,为构建高效智能的现代化电网,在实现碳达峰、碳中和目标过程中如何确保电网安全稳定运行至关重要.

现代电力系统大多由不同区域的子系统组合而成,利用负荷频率控制策略,不断调整发电机组输出有功功率,从而确保系统发电侧与用户需求侧的实时平衡[8]. 而控制方法的实现,依托于电力系统中不同传感器所获得的量测信息,这些信息经由通讯网络传输至控制器端以便于实时修正控制策略. 若系统信

收稿日期: 2021-08-31；**录用日期:** 2022-03-28.

基金项目: 国家自然科学基金项目(61973277)；浙江省自然科学基金项目(LR20F030004, LQ18F030005).

责任编委: 孙秋野.

†通讯作者. E-mail: bchen@zjut.edu.cn.

*本文附带电子附录文件,可登录本刊官网该文“资源附件”区自行下载阅览.

息受到FDI攻击并被恶意篡改,则控制决策中心难以估计系统运行状态,从而诱发电力安全事故. 针对电网中可能存在的恶意FDI攻击,已有许多攻击检测方法可以实现对攻击信号的快速预警. 例如: 文献[9]提出一种基于多元高斯分布的异常检测方法,通过电力系统测量单元所采集数据的相关特性,分别训练用于瞬态和稳态FDI攻击检测的多元高斯模型; 文献[10]基于电力系统安全能量管理单元采集的数据提出一种鲁棒检测方法实现FDI攻击检测; 文献[11]基于合取规则的多数表决算法协同检测向量测量单元遭受的FDI攻击信号,并设计了具有自适应置信度更新算法的向量测量单元以估计系统整体运行状态. 注意到上述方法只是检测系统是否遭受到FDI攻击,而电力系统在受到攻击时不但要检测攻击,更要保证在不停机的情况下持续安全生产电能. 在这种情况下,针对攻击信号的实时估计有助于防御方得到攻击的时域特征,进而设计简单有效的补偿措施以减小攻击的影响[12]. 现有安全状态估计大多采用集中式估计方法[13-17],其优点是当所有区域电力系统量测信息可得时,集中式状态估计方法能够保证最优估计性能. 但随着碳达峰、碳中和目标下新能源电网不断并入,新型电力系统日趋复杂. 由于通信协议和电力载波的约束[18],海量电网数据传输至集中处理中心时难免存在线路堵塞、接收延迟等问题[19]. 而分布式估计方法无需电网全局量测信息便能对不同区域的电力系统分别进行状态估计,能够有效避免传输庞大数据导致的通讯堵塞问题. 为此,文献[20]通过一种分布式未知输入观测器实现对各区域FDI攻击信号的估计; 文献[21]针对电力系统提出了一种最优两阶卡尔曼方法来估计电力系统的状态及FDI攻击信号. 然而,上述方法大多是基于量测信息绝对安全的条件下设计的,而传感器量测数据遭受恶意攻击时必然会损害估计性能. 因此,如何基于被攻击的量测信号来设计FDI攻击信号估计与系统状态估计更具挑战性.

另一方面,电力系统负荷频率控制下不可避免产生负载偏差,且一定程度影响系统估计性能. 现有文献将负载偏差建模为不确定性扰动,然后以鲁棒估计与控制方法来解决负荷频率控制系统中的负载偏差问题[22-23]. 虽然上述方法对负载偏差信号进行了一定处理,提高了电力系统状态估计的精准性,但其对系统运行的影响依旧不可忽略.

综上分析,为了解决FDI攻击下多区域互联电力系统的状态估计问题,本文提出一种基于分布式中间观测器的安全状态估计方法,可避免集中式估计方法存在传输数据量大、信息传输延迟的问题. 特别地,分布式中间观测器不需要满足系统严格正实条件或者观测器匹配条件. 所设计的分布式中间观测器能够同时估计不同区域的系统状态、FDI攻击信号以及负载偏差. 在此基础上,进一步设计补偿控制策略以降低FDI攻击和负载偏差对系统性能带来的负面影响.

1 预备知识

引理1 对于任意矩阵$X \in R^{n\times m}$和$Y \in R^{n\times s}$,存在$\mu > 0$使得以下不等式[24]成立:

$$X^{\mathrm{T}}Y + Y^{\mathrm{T}}X \leqslant \mu X^{\mathrm{T}}X + \frac{1}{\mu}Y^{\mathrm{T}}Y.$$

引理2 对于给定的对称矩阵

$$Q = \begin{bmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{bmatrix},$$

存在以下等价条件[25]:

1) $Q < 0$;

2) $Q_{11} < 0, Q_{22} - Q_{12}^{\mathrm{T}}Q_{11}^{-1}Q_{12} < 0$;

3) $Q_{22} < 0, Q_{11} - Q_{12}Q_{22}^{-1}Q_{12}^{\mathrm{T}} < 0$.

2 问题描述

2.1 互联电力系统的状态空间模型

大型电力系统是由多个区域的电力系统通过联络线组成,通过负荷频率控制保证各区域电力系统的稳定运行,一个两区域的负荷频率控制电力系统结构框图如图1所示.

根据图1,第i区域电力系统的涡轮阀位置偏差ΔP_{gi}同时受到区域输出的频率偏差Δf_i及参考点负载设定值ΔP_{ci}的影响,其动态方程[26]可表示为

$$\Delta\dot{P}_{gi}(t) = -\frac{1}{R_iT_{gi}}\Delta f_i(t) - \frac{1}{T_{gi}}\Delta P_{gi}(t) + \frac{1}{T_{gi}}\Delta P_{ci}(t). \quad (1)$$

其中: $i \in \{1,2,\dots,N\}$, N为电力系统子系统的个数; T_{gi}为调速器的时间常数; R_i为速度衰减系数. 同时,涡轮阀位置偏差ΔP_{gi}会影响机械功率偏差ΔP_{mi}, ΔP_{mi}的动态方程为

$$\Delta\dot{P}_{mi}(t) = -\frac{1}{T_{\mathrm{chi}}}\Delta P_{mi}(t) + \frac{1}{T_{\mathrm{chi}}}\Delta P_{gi}(t), \quad (2)$$

其中T_{chi}为涡轮机时间常数.

区域电力系统输出的频率偏差Δf_i不仅与机械功率偏差ΔP_{mi}有关,也与联络线的网系潮流$\Delta P_{\mathrm{tie}}^i$有关,同时受到子系统自身的负载偏差$\Delta P_{Li}$影响,其动态方程为

$$\Delta\dot{f}_i(t) = -\frac{D_i}{2H_i}\Delta f_i(t) + \frac{1}{2H_i}\Delta P_{mi}(t) - \frac{1}{2H_i}\Delta P_{tie}^i(t) - \frac{1}{2H_i}\Delta P_{Li}(t). \quad (3)$$

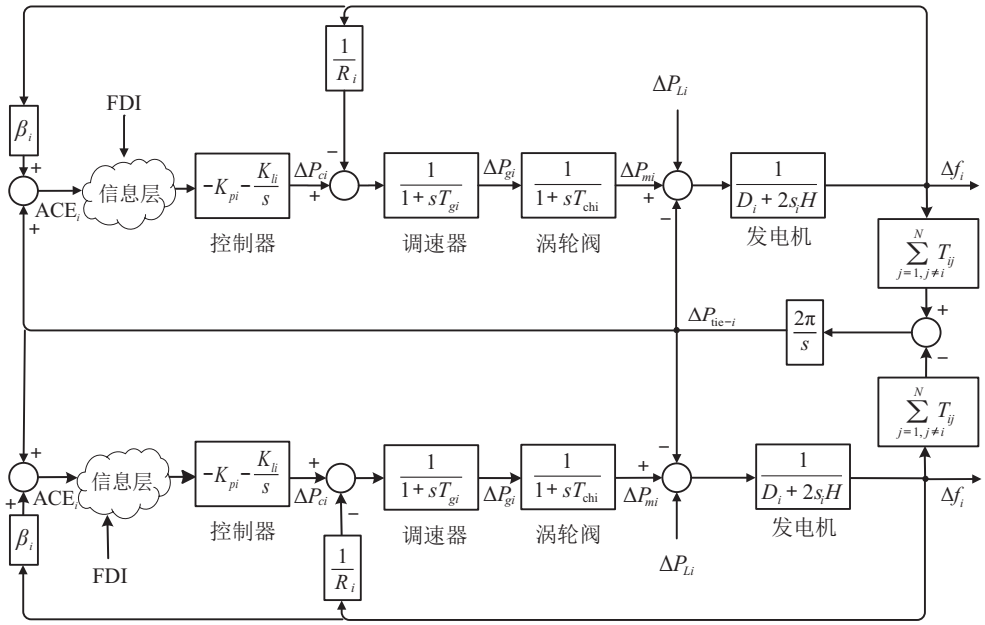

图 1　两区域电力系统结构框图

其中: H_i 为等效惯性常数, D_i 为等效阻尼系数. 区域传输线的网系潮流 $\Delta P^i_{\rm tie}$ 受各区域输出的频率偏差 Δf_i 影响,动态方程为

$$\Delta \dot{P}^i_{\rm tie}(t)=\sum_{j=1,j\neq i}^{N} 2\pi T_{ij}(\Delta f_i(t)-\Delta f_j(t)), \quad (4)$$

其中 T_{ij} 是同步功率系数.

基于区域的输出频率偏差 Δf_i 以及传输线的网系潮流 $\Delta P^i_{\rm tie}$, 各区域电力系统的区域控制误差信号 ${\rm ACE}_i$ 可表示为

$${\rm ACE}_i(t)=\beta_i\Delta f_i(t)+\Delta P^i_{\rm tie}(t), \quad (5)$$

其中 $\beta_i=1/R_i+D_i$.

然后,通过在系统中加入PI控制器,使得各子系统的输出保持稳定,即

$$\Delta P_{ci}(t)=-K_{Pi}{\rm ACE}_i(t)-K_{Ii}\int_0^t {\rm ACE}_i(s){\rm d}s, \quad (6)$$

其中 K_{Pi} 和 K_{Ii} 为控制器的增益系数.

定义各区域电力系统的状态 $x_i(t)={\rm col}\Big\{\Delta f_i(t), \Delta P_{mi}(t), \Delta P_{gi}(t), \Delta P^i_{\rm tie}(t), \int_0^t {\rm ACE}_i(s){\rm d}s\Big\}$, 量测 $y_i(t)={\rm col}\Big\{{\rm ACE}_i(t), \int_0^t {\rm ACE}_i(s){\rm d}s\Big\}$, 则第 i 区域的电力系统状态空间模型可表示为

$$\begin{aligned}&\dot{x}_i(t)=A_ix_i(t)+B_iu_i(t)+B_{wi}w_i(t)-\sum_{j=1}^{N}H_{ij}x_j(t),\\&y_i(t)=C_ix_i(t).\end{aligned} \quad (7)$$

其中

$$A_i=\begin{bmatrix}-\frac{D_i}{2H_i} & \frac{1}{2H_i} & 0 & -\frac{1}{2H_i} & 0\\ 0 & -\frac{1}{T_{\rm chi}} & \frac{1}{T_{\rm chi}} & 0 & 0\\ -\frac{1}{R_iT_{gi}} & 0 & -\frac{1}{T_{gi}} & 0 & 0\\ \sum_{j=1,j\neq i}^{N}2\pi T_{ij} & 0 & 0 & 0 & 0\\ \beta_i & 0 & 0 & 1 & 0\end{bmatrix},\ B_i=\begin{bmatrix}0\\0\\\frac{1}{T_{gi}}\\0\\0\end{bmatrix},\ B_{wi}=\begin{bmatrix}-\frac{1}{M_i}\\0\\0\\0\\0\end{bmatrix},\ H_{ij}=\begin{bmatrix}0&0&0&0&0\\0&0&0&0&0\\0&0&0&0&0\\-2\pi T_{ij}&0&0&0&0\\0&0&0&0&0\end{bmatrix},\ C_i=\begin{bmatrix}\beta_i&0\\0&0\\0&0\\1&0\\0&1\end{bmatrix}^{\rm T},$$

$u_i(t)=\Delta P_{ci}(t), w_i(t)=\Delta P_{Li}(t), H_{ij}$ 是与相邻区域电力子系统的耦合矩阵.

2.2　FDI攻击下的区域电力系统状态空间模型

传感器通过网络传输的量测数据可能遭到FDI攻击恶意篡改,进而影响系统状态估计与安全控制性能. 当 i 区域电力系统传输受到攻击时,定义 $a_{yi}(t)$ 为FDI攻击信号,此时该区域系统状态空间模型为

$$\begin{aligned}&\dot{x}_i(t)=A_ix_i(t)+B_iu_i(t)+B_{wi}w_i(t)-\sum_{j=1}^{N}H_{ij}x_j(t),\\&y_i(t)=C_ix_i(t)+E_ia_{yi}(t),\end{aligned} \quad (8)$$

其中E_i为适当维度的系数矩阵.

令$z_i(t)=\mathrm{col}\{x_i(t),a_{yi}(t)\}$,则式(8)等价于

$$\begin{cases}\dot{z}_i(t)=\bar{A}_iz_i(t)+\bar{B}_iu_i(t)-\sum\limits_{j=1}^{N}\bar{H}_{ij}z_j(t)+\\ \qquad\bar{B}_{wi}w_i(t)+M_i\dot{a}_{yi},\\ y_i(t)=\bar{C}_iz_i(t).\end{cases}\tag{9}$$

其中

$$\bar{A}_i=\begin{bmatrix}A_i&0\\0&0\end{bmatrix},\ \bar{B}_i=\begin{bmatrix}B_i\\0\end{bmatrix},\ \bar{B}_{wi}=\begin{bmatrix}B_{wi}\\0\end{bmatrix},$$

$$\bar{H}_{ij}=\begin{bmatrix}H_{ij}&0\\0&0\end{bmatrix},\ M_i=\begin{bmatrix}0\\I\end{bmatrix},\ \bar{C}_i=\begin{bmatrix}C_i&E\end{bmatrix}.$$

本文设计一种分布式安全状态估计方法,分别估计各区域电力子系统的状态、负载偏差信号及量测遭受的FDI攻击信号,并通过设计补偿控制策略降低负载偏差和FDI攻击对电力系统造成的影响.

注1 考虑实际电力系统中,负载偏差及量测数据具有连贯性强、极少出现数值跳变的特点,假设负载偏差信号及FDI攻击存在导数有界约束[27-28],即存在θ_1、θ_2使得$||\tilde{\dot{w}}(t)||\leqslant\theta_1$、$||\tilde{\dot{a}}_y(t)||\leqslant\theta_2$,其中$\theta_1$、$\theta_2$均为正且未知.

3 中间观测器及补偿控制策略的设计

本节首先通过构建中间变量设计一种分布式中间观测器;然后,给出电力系统估计误差方程状态一致渐近有界的条件;最后,设计补偿控制策略来降低负载偏差及FDI攻击信号对电力系统运行的影响.

3.1 中间观测器的设计

首先,定义中间变量σ_i[29]为

$$\sigma_i(t)=w_i(t)-k_i\bar{B}_{wi}^{\mathrm{T}}z_i(t),\tag{10}$$

其中k_i为可调标量,选取合适值以调整估计误差系统收敛速度.

由式(9)可得中间变量动态方程为

$$\begin{aligned}\dot{\sigma}_i(t)=&\\ &\dot{w}_i(t)-k_i\bar{B}_{wi}^{\mathrm{T}}\Big(\bar{A}_iz_i(t)+\bar{B}_iu_i(t)+\bar{B}_{wi}\sigma_i(t)+\\ &k_i\bar{B}_{wi}\bar{B}_{wi}^{\mathrm{T}}z_i(t)-\sum_{j=1}^{N}\bar{H}_{ij}z_j(t)+M_i\dot{a}_{yi}(t)\Big).\end{aligned}\tag{11}$$

设计i区域电力系统的分布式中间观测器为

$$\begin{aligned}\dot{\hat{z}}_i(t)=&\bar{A}_i\hat{z}_i(t)+\bar{B}_{wi}\hat{w}_i(t)-\sum_{j=1}^{N}\bar{H}_{ij}\hat{z}_j(t)+\\ &\bar{B}_iu_i(t)+L_i(y_i(t)-\bar{C}_i\hat{z}_i(t)),\end{aligned}\tag{12}$$

$$\begin{aligned}\dot{\hat{\sigma}}_i(t)=&-k_i\bar{B}_{wi}^{\mathrm{T}}\Big(\bar{A}_i\hat{z}_i(t)+\bar{B}_iu_i(t)+\bar{B}_{wi}\hat{\sigma}_i(t)+\\ &k_i\bar{B}_{wi}\bar{B}_{wi}^{\mathrm{T}}\hat{z}_i(t)-\sum_{j=1}^{N}\bar{H}_{ij}\hat{z}_j(t)\Big).\end{aligned}\tag{13}$$

则电力系统全局估计方程如下:

$$\dot{\hat{z}}(t)=\tilde{A}\hat{z}(t)+\tilde{B}u(t)+\tilde{B}_w\hat{w}(t)+\tilde{L}(y(t)-\hat{y}(t)),\tag{14}$$

$$\begin{aligned}\dot{\hat{\sigma}}(t)=&-k\tilde{B}_w^{\mathrm{T}}\tilde{B}_w\hat{\sigma}(t)-k\tilde{B}_w^{\mathrm{T}}\tilde{A}\hat{z}(t)-k\tilde{B}_w^{\mathrm{T}}\tilde{B}u(t)-\\ &k^2\tilde{B}_w^{\mathrm{T}}\tilde{B}_w\tilde{B}_w^{\mathrm{T}}\hat{z}(t).\end{aligned}\tag{15}$$

其中

$\tilde{C}=\mathrm{diag}\{\bar{C}_1,\dots,\bar{C}_N\}$, $\tilde{B}_w=\mathrm{diag}\{\bar{B}_{w1},\dots,\bar{B}_{wN}\}$,

$\tilde{B}=\mathrm{diag}\{\bar{B}_1,\dots,\bar{B}_N\}$, $\tilde{M}=\mathrm{diag}\{M_1,\dots,M_N\}$,

$\tilde{L}=\mathrm{diag}\{L_1,\dots,L_N\}$, $k=\mathrm{diag}\{k_1,\dots,k_N\}$,

$\hat{z}(t)=[\hat{z}_1^{\mathrm{T}}(t),\dots,\hat{z}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, $\hat{w}(t)=\big[\hat{w}_1^{\mathrm{T}}(t),\dots,\hat{w}_N^{\mathrm{T}}(t)\big]^{\mathrm{T}}$,

$\hat{\sigma}(t)=[\hat{\sigma}_1^{\mathrm{T}}(t),\dots,\hat{\sigma}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, $u(t)=[u_1^{\mathrm{T}}(t),\dots,u_N^{\mathrm{T}}(t)]^{\mathrm{T}}$,

$y(t)=[y_1^{\mathrm{T}}(t),\dots,y_N^{\mathrm{T}}(t)]^{\mathrm{T}}$, $\hat{y}(t)=[\hat{y}_1^{\mathrm{T}}(t),\dots,\hat{y}_N^{\mathrm{T}}(t)]^{\mathrm{T}}$,

$\tilde{A}=[\bar{A}_{ij}]_{N\times N}$, $\bar{A}_{ij}=\bar{H}_{ij}$, $\bar{A}_{ii}=\bar{A}_i$.

此时,由式(9)和(11)可得全局电力系统及中间变量的动态方程为

$$\dot{z}(t)=\tilde{A}z(t)+\tilde{B}u(t)+\tilde{B}_ww(t)+\tilde{M}\dot{a}_y(t),\tag{16}$$

$$\begin{aligned}\dot{\sigma}(t)=&-k\tilde{B}_w^{\mathrm{T}}\tilde{B}_w\sigma(t)-k\tilde{B}_w^{\mathrm{T}}\tilde{A}z(t)-k\tilde{B}_w^{\mathrm{T}}\tilde{B}u(t)-\\ &k\tilde{B}_w^{\mathrm{T}}\tilde{M}\dot{a}_y(t)-k^2\tilde{B}_w^{\mathrm{T}}\tilde{B}_w\tilde{B}_w^{\mathrm{T}}z(t)+\dot{w}(t).\end{aligned}\tag{17}$$

定义估计误差$e_z(t)=z(t)-\hat{z}(t)$, $e_\sigma(t)=\sigma(t)-\hat{\sigma}(t)$, $e_w(t)=w(t)-\hat{w}(t)$, $e_y(t)=y(t)-\hat{y}(t)$,则有

$$e_w(t)=e_\sigma(t)+k\tilde{B}_w^{\mathrm{T}}e_z(t).\tag{18}$$

全局估计误差系统为

$$\begin{aligned}\dot{e}_z(t)=&(\tilde{A}-\tilde{L}\tilde{C})e_z(t)+\tilde{B}_we_\sigma(t)+\\ &k\tilde{B}_w\tilde{B}_w^{\mathrm{T}}e_z(t)+\tilde{M}\dot{a}_y(t),\end{aligned}\tag{19}$$

$$\begin{aligned}\dot{e}_\sigma(t)=&-k\tilde{B}_w^{\mathrm{T}}\tilde{B}_we_\sigma(t)-k\tilde{B}_w^{\mathrm{T}}\tilde{A}e_z(t)-\\ &k^2\tilde{B}_w^{\mathrm{T}}\tilde{M}\dot{a}_y(t)-k^2\tilde{B}_w^{\mathrm{T}}\tilde{B}_w\tilde{B}_w^{\mathrm{T}}e_z(t)+\dot{w}(t).\end{aligned}\tag{20}$$

定理1 对于给定的$k>0$、$\delta>0$,若存在对称矩阵$P_1>0$、$P_2>0$以及块对角矩阵G使得如下不等式成立:

$$\begin{bmatrix}\Omega_{11}&\Omega_{12}&P_1M&0&0\\*&\Omega_{22}&0&kP_2\tilde{B}_w^{\mathrm{T}}M&P_2\\*&*&-\delta I&0&0\\*&*&*&-\delta I&0\\*&*&*&*&-\delta I\end{bmatrix}<0,\tag{21}$$

则所有子区域电力系统估计误差为一致渐近有界,且i区域分布式中间观测器增益为$L_i=P_{1i}^{-1}G_i$. 其中

$$\Omega_{11}=(P_1\tilde{A}-G\tilde{C}+kP_1\tilde{B}_w\tilde{B}_w^{\mathrm{T}})+(P_1\tilde{A}-G\tilde{C}+kP_1\tilde{B}_w\tilde{B}_w^{\mathrm{T}})^{\mathrm{T}},$$

$$\Omega_{12}=P_1\tilde{B}_w-k\tilde{A}^{\mathrm{T}}\tilde{B}_wP_2-k^2\tilde{B}_w\tilde{B}_w^{\mathrm{T}}\tilde{B}_wP_2,$$

$$\Omega_{22}=-kP_2\tilde{B}_w^{\mathrm{T}}\tilde{B}_w-(kP_2\tilde{B}_w^{\mathrm{T}}\tilde{B}_w)^{\mathrm{T}}.$$

限于篇幅,证明略.

3.2　补偿控制策略设计

FDI 攻击下,i 区域电力闭环控制系统为

$$\dot{x}_i(t)=A_ix_i(t)+B_i(K_iy_i(t)+E_ia_{yi}(t))+B_{wi}w_i(t)-\sum_{j=1}^{N}H_{ij}x_j(t). \tag{22}$$

显然,一般 PI 控制策略无法解决攻击信号 $a_{yi}(t)$ 对系统状态的影响. 因此,根据上述分布式中间观测器的研究成果,可设计如下补偿控制输入:

$$u_a(t)=K_iy_i(t)-K_iE_i\hat{a}_{yi}(t)-(B_i^{\mathrm{T}}B_i)^{-1}B_i^{\mathrm{T}}B_{wi}\hat{w}_i(t). \tag{23}$$

补偿策略下区域子系统方程为

$$\dot{x}_i(t)=A_ix_i(t)+B_iK_i(y_i(t)+E_ia_{yi}(t)-E_i\hat{a}_{yi}(t))+B_{wi}(w_i(t)-\hat{w}_i(t))-\sum_{j=1}^{N}H_{ij}x_j(t). \tag{24}$$

由上述方程可知,当本文设计的分布式中间观测器能准确重构 FDI 攻击信号与负载偏差时,补偿输入可以实时并充分抵消其两者对多区域电力系统安全运行的影响.

注 2　分布式中间观测器的设计实现了对各区域电力系统状态、负载偏差及 FDI 攻击信号的同时估计,有效地避免了集中式安全估计方法存在的信息传输量大、传输延迟问题,以及随着系统规模扩张所带来的 LMI 无解问题. 特别地,分布式中间观测器不需要系统满足严格正实条件或观测器匹配条件[30-31],通过中间变量即可实现观测器收敛速度的调节.

4　仿真验证

考虑一个 8 区域电力系统的仿真算例,其拓扑结构如图 2 所示,且各区域的具体参数[32] 如下:

区域 1、3、5、7: $T_{\mathrm{chi}}=0.17\,\mathrm{s}, T_{gi}=0.4\,\mathrm{s}, D_i=1.5, R_i=0.05, M_i=12, \beta_i=41.5, T_{ij}=0.05.$

区域 2、4、6、8: $T_{\mathrm{chi}}=0.2\,\mathrm{s}, T_{gi}=0.35\,\mathrm{s}, D_i=1.8, R_i=0.05, M_i=12, \beta_i=61.8, T_{ij}=0.05.$

当区域 3 量测数据传输受到 FDI 攻击时,考虑负载偏差与攻击信号如表 1 所示. 通过 Matlab 中的 LMI 工具箱求解线性矩阵不等式(21),得到分布式中间观测器的增益矩阵 L_i,设计分布式中间观测器对区域电力系统进行安全状态估计.

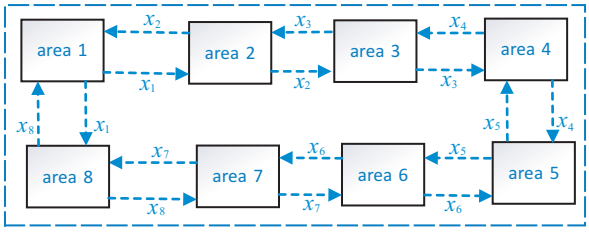

图 2　8 区域互联电力系统

表 1　FDI 攻击信号及负载偏差

t/s	[0, 15)	[15, 25)	[25, 45)	[45, 80)
$a_{y3}(t)$	0	$0.5t$	0	$2\sin(0.2t)$
t/s	[0, 5)	[5, 35)	[35, 57)	[57, 80)
$w_3(t)$	0	$0.1t$	1	$\sin(0.5t)$

分布式中间观测器估计结果如图 3、图 4 所示. 由图 3 可知: 针对系统中存在的负载偏差,本文所设计的分布式中间观测器具有较好的估计性能; 当负载偏差变化较大时,估计误差仍能迅速收敛至 0 附近. 由图 4 可知: 分布式中间观测器对于电力系统量测数据遭受的 FDI 攻击,能精确地重构攻击信号,保

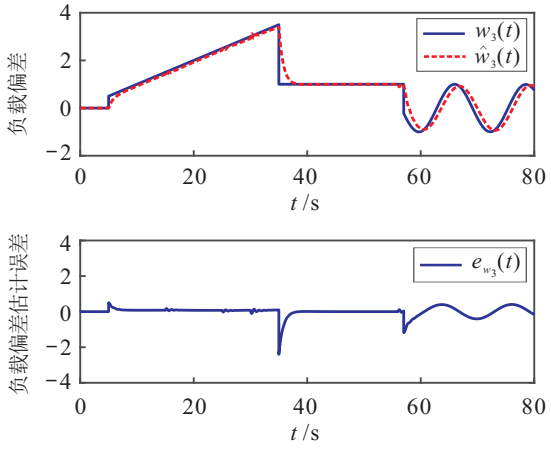

图 3　负载偏差估计及误差

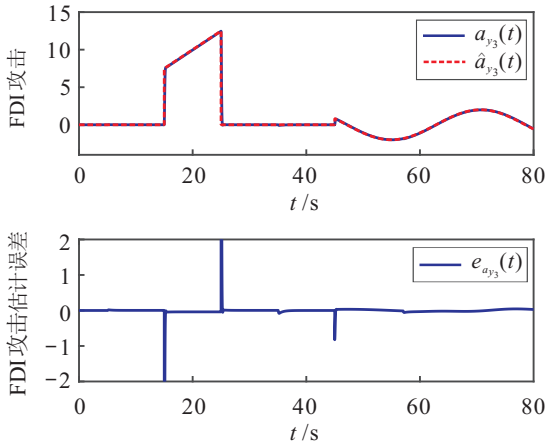

图 4　FDI 攻击信号估计及误差

证一定的攻击估计性能;同样地,当FDI攻击信号变化较大时,中间观测器依然具有快速收敛的能力. 特别地,不同k_i值下的分布式中间观测器估计性能如图5所示,k_i值的选取影响分布式中间观测器的收敛速度.

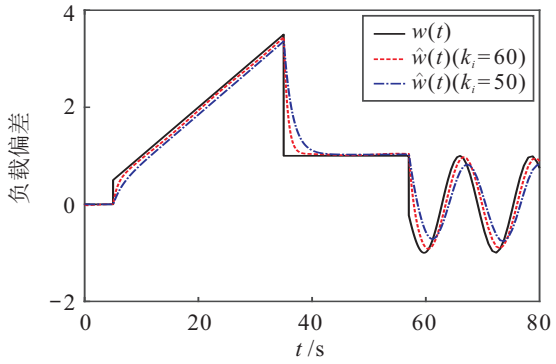

图5 不同k_i时的负载偏差估计

由于在8区域电力系统下集中式中间观测器存在LMI无解的情况,以4区域电力系统的负载偏差估计为例,将本文所提出的分布式中间观测器与集中式方法[9]以及分布式故障观测器方法[33]进行比较. 在不考虑集中式估计中可能出现的冗余信息传输延迟的情况下,图6给出3种方法的估计性能对比. 相较于依赖全局信息的集中式中间观测器,分布式中间观测器在仅依赖当前区域及相邻区域的信息的情况下,仍然能够实现对负载偏差的准确估计. 同时,相较于分布式故障观测器,分布式中间观测器具有更好的估计性能.

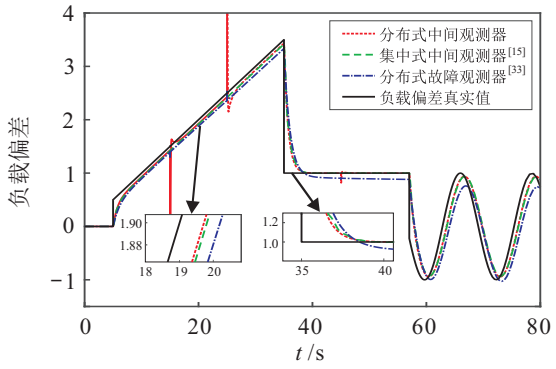

图6 负载偏差估计对比

根据上述分布式中间观测器估计结果,由式(23)可设计补偿控制输入以降低FDI攻击及负载偏差对系统状态的影响. 图7给出了补偿前后3区域电力系统状态(机械功率偏差与涡轮阀位置偏差)分布情况. 显然,原PI控制下的3区域电力系统受到FDI攻击时偏离稳定状态. 相比于原机械功率与涡轮阀位置偏差值,补偿控制输入下的偏差值更靠近0值附近. 因此,验证了本文所提出分布式中间观测器方法与补偿控制策略的有效性.

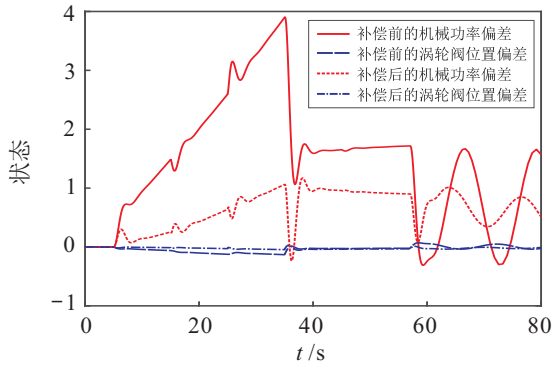

图7 补偿前后区域3部分状态对比

5 结 论

针对负荷频率控制下的多区域电力系统遭受FDI攻击的情况,本文提出了一种分布式中间观测器,分别对各区域电力子系统进行安全状态估计. 分布式中间观测器能够在系统不满足严格正实条件或观测器匹配条件的情况下,同时估计每个区域的状态、FDI攻击信号及负载偏差. 最后,根据分布式中间观测器的估计结果,设计了补偿控制策略以对电力系统进行实时补偿,保证电力系统的稳定运行. 仿真结果验证了所提出方法的有效性.

参考文献(References)

[1] Wu J, Li Y N, Li S Y. State estimation for distributed cyber-physical power systems under data attacks[J]. Control and Decision, 2016, 31(2): 331-336.

[2] Chen C Y, Zhou Y, Chi M, et al. Review of large power grid vulnerability based on complex network theory[J]. Control and Decision, 2022, 37(4): 782-798.

[3] Chen J, Dou C X, Xiao L, et al. Fusion state estimation for power systems under DoS attacks: A switched system approach[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 49(8): 1679-1687.

[4] Lou X, Tran C, Tan R, et al. Assessing and mitigating impact of time delay attack: Case studies for power grid controls[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(1): 141-155.

[5] Hu M N, Chen B, Yu L. Hidden FDI attack strategy for distributed least square estimation[J]. Control and Decision, 2021, 36(8): 1963-1969.

[6] Shi J Y, Liu S C, Chen B, et al. Distributed data-driven intrusion detection for sparse stealthy FDI attacks in smart grids[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68(3): 993-997.

[7] Zhou J, Chen B, Yu L. Intermediate-variable-based estimation for FDI attacks in cyber-physical systems[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(11): 2762-2766.

[8] Yang L, Sun Y Z, Xu J, et al. Adaptive load frequency control of wind power system based on online

reinforcement learning[J]. Automation of Electric Power Systems, 2020, 44(12): 74-83.

[9] An Y, Liu D. Multivariate Gaussian-based false data detection against cyber-attacks[J]. IEEE Access, 2019, 7: 119804-119812.

[10] Zhao J B, Mili L, Wang M. A generalized false data injection attacks against power system nonlinear state estimator and countermeasures[J]. IEEE Transactions on Power Systems, 2018, 33(5): 4868-4877.

[11] Li B B, Lu R X, Wang W, et al. Distributed host-based collaborative detection for false data injection attacks in smart grid cyber-physical system[J]. Journal of Parallel and Distributed Computing, 2017, 103: 32-41.

[12] Weng P D, Chen B, Yu L. Fusion estimate of FDI attack signals[J]. Acta Automatica Sinica, 2021, 47(9): 2292-2300.

[13] Weng S Q, Zhou J, Chen B, et al. Secure intermediate-variable-based estimation for multi-area power systems under FDI attacks[C]. 2021 International Conference on Control, Automation and Information Sciences (ICCAIS). Xi'an, 2021: 608-613.

[14] Ye J, Yu X. Detection and estimation of false data injection attacks for load frequency control systems[J]. Journal of Modern Power Systems and Clean Energy, 2022, 10(4): 861-870.

[15] Xu J, Lum K Y, Loh A P. A gain-varying UIO approach with adaptive threshold for FDI of nonlinear F16 systems[J]. Journal of Control Theory and Applications, 2010, 8(3): 317-325.

[16] Kazemi Z, Safavi A A, Naseri F, et al. A secure hybrid dynamic-state estimation approach for power systems under false data injection attacks[J]. IEEE Transactions on Industrial Informatics, 2020, 16(12): 7275-7286.

[17] Haes Alhelou H, Hamedani Golshan M E, Hatziargyriou N D. Deterministic dynamic state estimation-based optimal LFC for interconnected power systems using unknown input observer[J]. IEEE Transactions on Smart Grid, 2020, 11(2): 1582-1592.

[18] Chen B, Hu G Q, Ho D W C, et al. Distributed estimation and control for discrete time-varying interconnected systems[J]. IEEE Transactions on Automatic Control, 2022, 67(5): 2192-2207.

[19] Wen S P, Yu X H, Zeng Z G, et al. Event-triggering load frequency control for multiarea power systems with communication delays[J]. IEEE Transactions on Industrial Electronics, 2016, 63(2): 1308-1317.

[20] Khalghani M R, Solanki J, Solanki S K, et al. Resilient frequency control design for microgrids under false data injection[J]. IEEE Transactions on Industrial Electronics, 2021, 68(3): 2151-2162.

[21] Tummala A S L V, Inapakurthi R K. A two-stage Kalman filter for cyber-attack detection in automatic generation control system[J]. Journal of Modern Power Systems and Clean Energy, 2022, 10(1): 50-59.

[22] Liu J L, Gu Y Y, Zha L J, et al. Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 49(8): 1665-1678.

[23] Khalghani M R, Solanki J, Khushalani Solanki S, et al. Stochastic secondary frequency control of islanded microgrid under uncertainties[J]. IEEE Systems Journal, 2021, 15(1): 1056-1065.

[24] Jabbari F, Benson R W. Observers for stabilization of systems with matched uncertainty[J]. Dynamics and Control, 1992, 2(3): 303-323.

[25] Zhan F Z. The schur complement and its applications[M]. New York: Springer, 2005: 47-60.

[26] Bevrani H. Robust power system frequency control[M]. New York: Springer, 2009: 34-46.

[27] Abbaspour A, Sargolzaei A, Forouzannezhad P, et al. Resilient control design for load frequency control system under false data injection attacks[J]. IEEE Transactions on Industrial Electronics, 2020, 67(9): 7951-7962.

[28] Bi W J, Zhang K F, Yuan K, et al. Observer-based attack detection and mitigation for load frequency control system[C]. 2019 IEEE Power & Energy Society General Meeting. Atlanta, 2019: 1-5.

[29] Zhu J W. Research on fault diagnosis and fault tolerant control via intermediate estimator[D]. Shenyang: Northeastern University, 2016.

[30] Lozano-Leal R, Joshi S M. Strictly positive real transfer functions revisited[C]. The 29th IEEE Conference on Decision and Control. Honolulu, 1990: 3640-3641.

[31] Dhahri S, Hmida F B, Sellami A, et al. Actuator fault reconstruction for linear uncertain systems using sliding mode observer[C]. The 3rd International Conference on Signals, Circuits and Systems (SCS). Medenine: IEEE, 2009: 1-6.

[32] Liu S C, Liu P X. Distributed model-based control and scheduling for load frequency regulation of smart grids over limited bandwidth networks[J]. IEEE Transactions on Industrial Informatics, 2018, 14(5): 1814-1823.

[33] Zhang K, Jiang B, Chen M, et al. Distributed fault estimation and fault-tolerant control of interconnected systems[J]. IEEE Transactions on Cybernetics, 2021, 51(3): 1230-1240.

作者简介

翁世清 (1995−), 男, 硕士生, 从事电力信息物理系统安全的研究, E-mail: wengshiqing02@163.com;

翁品迪 (1996−), 男, 博士生, 从事信息物理系统中攻击信号的融合检测的研究, E-mail: pwd2gg@aliyun.com;

周京 (1993−), 男, 博士生, 从事信息物理系统安全的研究, E-mail: jzhou@zjut.edu.cn;

陈博 (1984−), 男, 教授, 博士生导师, 从事信息融合、安全估计与控制等研究, E-mail: bchen@zjut.edu.cn;

苏子漪 (1982−), 女, 讲师, 博士, 从事信号处理、鲁棒控制等研究, E-mail: ziyi_su@vip.163.com.