文章编号: 1001-0920 (2016) 02-0331-06 **DOI:** 10.13195/j.kzyjc.2014.1748

分布式电网CPS系统数据攻击下的状态估计

邬 晶, 李依宁, 李少远

(上海交通大学 自动化系, 上海 200240)

摘 要: 电力物理网络通过构建信息网络进行优化调控并构成信息物理融合系统, 实现大规模分布式系统的优化控制, 随之而来的问题是病毒、黑客入侵、拒绝服务等来自信息网络的威胁, 导致物理系统恶意破坏. 鉴于此, 以攻击可检测为前提, 建立攻击信号下的电力系统分布式动态模型, 设计动态状态估计器检测受攻击的信号, 并估计其原始信号. 最后通过3机9节点分布式电网系统仿真实验验证了所设计的状态估计器对于数据攻击检测的有效性.

关键词: 信息物理系统; 数据攻击; 分布式状态估计

中图分类号: TP273 **文献标志码:** A

State estimation for distributed cyber-physical power systems under data attacks

WU Jing, *LI Yi-ning*, *LI Shao-yuan*

(Department of Automation, Shanghai Jiaotong University, Shanghai 200240, China. Correspondent: LI Yi-ning, E-mail: smilelyn@sjtu.edu.cn)

Abstract: For the physical network, such as the power physical network, the cyber network is built to optimize the regulation and control to constitute the cyber-physical system, in order to achieve optimal control of large scale distributed systems, which brings along with virus, hacking, denial of service from the threat of cyber network may lead to malicious damage in physical system. A distributed dynamic model for a class of power systems with data attack is built with the assumption of attack detectability. Dynamic state estimators are presented to detect the attacked data and estimate its original value. Finally, a simulation of the 9-bus distributed power system shows the effectiveness of the detection of the data attack by the proposed state estimators.

Keywords: cyber-physical systems; data attack; distributed state estimation

0 引 言

随着通信网络技术与嵌入式开发水平的不断提高, 信息物理融合系统(CPS)已在多个控制领域, 如电网控制、水网控制等工业控制过程中形成并产生深远影响. 该系统借助传感器或制动器量测和传送信息, 通过网络连接和人机接口实现交流. 随着其性能的增强和联网程度的提高, 迫切需要新的技术和方法满足它在安全和保护上的需求. 智能电网作为典型的信息物理融合系统, 伴随着电力系统智能化进程的加快, 电力物理网络与信息网络耦合性的增强, 未来对于电网安全运行的保护机制除了对物理元件的故障排查之外, 还要加强对通信层面数据攻击的监控, 以确保智能电网能够在整合物理过程、计算资源和通信能力的基础上进行流程监控和过程控制[1]. 电力系统状态估计正是实现对电网中数据攻击检测和安全防护的一种有效解决方案, 它通过监控与数据采集(SCADA)系统获取实时量测数据, 按照相应的估计算法得到系统状态的最佳估计值, 并将其输入到数据库中供其他计算分析程序使用.

现有的电力系统安全评估方法通常为静态估计方法, 如快速分解算法[2]、抗差最小二乘算法[3]和等效电流量测变换法[4]等. 其中文献[2]提出了对增广的雅克比矩阵进行Givens行变换的方法, 并将该方法应用于快速分解状态估计算法中坏数据的检测和辨识; 文献[3]在传统最小二乘估计方法的基础上描述了一种抗差最小二乘方法, 即通过等价权将抗差估计原理与最小二乘形式相结合, 在保证基本效率的基础上减小估值粗差的影响; 文献[4]通过将雅克比矩

收稿日期: 2014-11-17; **修回日期:** 2015-07-13.

基金项目: 国家自然科学基金项目(61233004, 61473184).

作者简介: 邬晶(1979−), 女, 副教授, 从事网络化控制系统与无线传感器等研究; 李依宁(1992−), 女, 硕士生, 从事智能电网控制的研究.

阵实现完全常数化, 进而实现信息矩阵的自动解耦. 但是, 随着电力系统的互联, 电力系统的规模越来越大, 以上所提到的集中式算法越来越无法满足当前电力系统实时性和结构多样性的要求, 并会导致收集的数据存在大量的不确定性. 因此, 近几年来出现了分布式的状态估计方法. 文献[5]提出了基于结构和电压等级分布的分布式抗差最小方差估计方法, 文献[6]提出了分布式标量加权融合稳态满阶的分布式卡尔曼滤波方法. 在这些方法的基础上, 文献[7]提出了一种基于等值网等值量测修正思想的分布式状态估计算法, 可在子系统本地获得全网计算效果, 并避免了同步等待问题. 这些分布式状态估计方法虽然在一定程度上解决了状态估计算法的复杂度和准确度问题, 但是没有充分利用系统的动态信息. 随着攻击者的攻击手段越来越隐秘以及发起攻击入口的随意性, 静态状态估计方法的局限性也逐渐显现出来, 特别是当攻击者对于系统网络结构完全掌握时, 无法通过静态状态估计方法检测到攻击信号[8-9]. 由于硬件技术与通信带宽的限制, 该算法在动态系统中的优化设计还处于起步阶段, 随着电力系统中相关硬件技术的提高, 如相位量测单元(PMUs)以及通信带宽的上升, 可利用的动态信息越来越丰富, 动态估计算法的研究开始引起国内外学者的广泛关注.

本文针对智能电网中的数据攻击检测问题, 提出一类动态分布式状态估计算法. 首先给出数据攻击下的智能电网分布式动态数学模型, 基于该数学模型分析攻击的可检测性, 并在此前提下设计一类动态分布式状态估计器. 该估计器能够检测数据是否受到攻击, 并及时将检测信息反馈到控制中心. 最后通过仿真算例表明了所提出方法的有效性.

1 数据攻击下电力系统分布式模型描述

CPS是一个综合数据计算、信息网络和物理环境的多维复杂系统, 通常表现为分布式系统. 其各个子系统要通过有线或无线的通信方式相互协调工作, 并借助传感器或制动器量测和传送信息, 通过网络连接和人机接口实现交流. 在该系统信息交互的过程中, 容易受到来自互联网等通讯层面的数据攻击, 进而破坏物理环境. 以智能电网为例, 当电网SCADA数据采集系统稳定运行时, 若此时系统内的某处量测单元或用户端负荷节点受到具有一定目的性的未知信号的干扰, 则这种干扰会带来系统一段时间的大幅震荡甚至发散的不稳定影响, 最终破坏电网的底层物理结构. 这种强行输入到系统内的未知信号称为电网的数据攻击信号, 表现在通信方面为数据丢包或原有数据重放等形式.

攻击信号用$u_K(t)$表示, 其中K表示攻击点的个数, 即攻击规模. 图1为存在数据攻击信号系统的分布式系统框图. 数据攻击a为状态攻击信号, 用$u_B(t)$表示, 其攻击点位于系统调控中心至电力网络运行状态之间的数据通信区域, 表现为电力系统控制过程中的数据拦截攻击等; 数据攻击b为输出攻击信号, 用$u_D(t)$表示, 其攻击点位于电力网络节点量测单元至系统调控中心的数据通信区域, 表现为量测值传输过程中的通信安全问题.

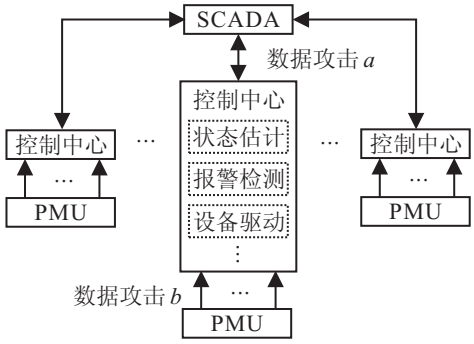


图1 数据攻击下的分布式系统框图

执行机构、控制对象和量测单元共同构成了数据攻击下智能电网的数学模型, 其分布式系统模型为

$$E_i\dot{x}_i(t)=A_ix_i(t)+\sum_{j=1,j\neq i}^{N}A_{ij}x_j(t)+B_{Ki}u_{Ki}(t),$$

$$y_i(t)=C_ix_i(t)+D_{Ki}u_{Ki},\ i\in\{1,2,\cdots,N\}. \quad (1)$$

其中: $x_i=[\delta_i\ \ \omega_i\ \ \theta_i]^{\mathrm{T}}$为第$i$个子系统内的状态变量, δ_i为发电机转子角, ω_i为发电机转子角速度, θ_i为负荷端相位角; $x_j=[\delta_j\ \ \omega_j\ \ \theta_j]^{\mathrm{T}}$为第$j$个子系统内的状态变量; y_i为第i个子系统内的量测单元输出; $B_{Ki}u_{Ki}(t)$为子系统内状态攻击信号; $D_{Ki}u_{Ki}(t)$为子系统内输出攻击信号; E_i为发电机传输特性矩阵; A_{ij}为与第i个子系统相连且连接方向为流入的第j个子区域状态变换模型; C_i为观测模型. 设电网第i个子系统内存在的传感器有p个, 发电机和发电机终端总线分别为n个, 输出端(即用户负荷线端数目)为m个, 则$x_i(t)\in R_n$, $u_{Ki}(t)\in R_m$, $y_i(t)\in R_p$, $E_i\in R_{n\times n}$, $A_{ij}\in R_{n\times n}$, $B_{Ki}\in R_{n\times m}$, $C_i\in R_{p\times n}$, $D_{Ki}\in R_{p\times m}$.

假设1 若第i个子系统和与之存在联系的第j个子系统的物理结构特性已知, 则E_i、A_i、C_i、A_{ij}已知.

假设2 若第i个子系统与第j个子系统存在联系, 则表示第i个子系统与第j个子系统存在功率流入的关系, $A_{ij}\neq 0$.

假设3 (E_i,A_i)正则, 且(E_i,A_i,C_i)可观.

假设4 因讨论该分布式电网系统的数据攻击

检测问题, 故系统内控制信号输入 $u_c(t)$ 可计于 $u_K(t)$ 内, 即 $u_K(t)$ 为 $u_c(t)$ 作用后的数据攻击信号.

针对该数据攻击下电力系统的分布式动态模型分析攻击的可检测性, 并在此前提条件下设计一类动态分布式状态估计器, 通过对未攻击时原始信号的预估, 实现对模型中数据攻击信号的检测.

2　攻击的可检测性分析

侵入信息物理融合系统的数据攻击通常采用某种特定的攻击策略以达到最佳的攻击效果. 设 $K \in \{1,2,\cdots,n+p\}$ 为攻击范围, 对于 $\forall i \in K$, 均存在某一时刻 t 使得 $u_i(t) \neq 0$; 对于 $\forall j \notin K$, 在任意时刻 t 有 $u_j(t)=0$.

数据攻击的通常模式有静态隐秘攻击、重放攻击、转换攻击和动态虚假数据注入攻击等. 根据不同的攻击模式, 给出攻击能否被检测的充分条件.

引理 1 (攻击可检测性)　x_i 为第 i 个子区域内状态变量的拉普拉斯表示, $\widetilde{x}_j$ 为除第 i 个子区域外其他所有子区域内状态变量列排列组成的列向量拉普拉斯表示, g_{Ki} 为第 i 个子区域内攻击向量的拉普拉斯表示, $\widetilde{A}_{ij}$ 为除第 i 个子区域外其他子区域对应的状态变换模型行排列组成的行向量. 若 g_{Ki} 满足

$$\begin{bmatrix} sE_i - A_i & -\widetilde{A}_{ij} & -B_{Ki} \\ C_i & 0 & D_{Ki} \end{bmatrix} \begin{bmatrix} x_i \\ \widetilde{x}_j \\ g_{Ki} \end{bmatrix} = 0, \quad (2)$$

则 g_{Ki} 对于式 (1) 而言是不可检测的.

证明　在分布式系统模型 (1) 中, 存在初始状态 $x_{i1}(0)$、$x_{i2}(0)$ 和攻击范围 K', 使得第 i 个子系统内的攻击信号表示为 $u_{K'}(t)$. 若该攻击范围 K' 下的攻击信号对电网的攻击效果无法通过量测单元辨识出来, 则不可检测. 对于 $\forall t$ 而言, 有

$$y_i(x_{i1}(0), u_{K'}(t), t) = y_i(x_{i2}(0), 0, t). \quad (3)$$

由于式 (1) 是线性的, 可以将式 (3) 改写成

$$y_i(x_{i1}(0), u_{K'}(t), t) = 0. \quad (4)$$

将式 (4) 代入系统分布式模型 (1) 中, 对于子区域某初始状态 $x_i(0) = x_{i1}(0) - x_{i2}(0)$, 若存在攻击信号 $u_{Ki}(t) = u_{K'}(t)$, 满足

$$\begin{aligned} &E_i\dot{x}_i(t) = \\ &A_i x_i(t) + \sum_{j=1, j\neq i}^{N} A_{ij}x_j(t) + B_{Ki}u_{Ki}(t), \\ &0 = C_i x_i(t) + D_{Ki}u_{Ki},\ i \in \{1,2,\cdots,N\}, \end{aligned} \quad (5)$$

则该攻击范围下的攻击信号 $u_{Ki}(t)$ 不可检测, 除此之外均可检测. 最后将式 (5) 拉氏变换并整理后得到 (2). □

3　分布式状态估计器设计

在集中式和分散式状态估计器[10-11]的基础上, 针对分布式结构的动态系统, 设计一种分布式动态状态估计算法, 并给出相关证明. 考虑如下形式的状态估计器:

$$\begin{aligned} &E_i\dot{\hat{x}}_i(t) = \\ &(A_i + G_iC_i)\hat{x}_i(t) + \sum_{j\in N_i^{in}} A_{ij}\hat{x}_j(t) - G_iy_i(t), \\ &r_i(t) = y_i(t) - C_i\hat{x}_i(t),\ i \in \{1,2,\cdots,N\}. \end{aligned} \quad (6)$$

其中: $\hat{x}_i(0) \in R_n$ 为第 i 个子系统内的状态估计值, $G_i \in R^{n\times p}$ 为状态观测矩阵, $r_i(t) \in R_p$ 为状态估计器输出的估计差值.

定理 1　对于分布式动态模型 (1) 和状态估计器 (6), 当且仅当 $u_{Ki}(t) = 0$ 时, $r_i(t) = 0$, 需满足 $(E_i, A_i + G_iC_i)$ 为正则且赫尔维茨稳定, 且

$$\rho((j\omega E_i - A_i - G_iC_i)^{-1}\tilde{A}_{ij}) < 1,\ \forall\omega \in R. \quad (7)$$

其中: 已知系统初始状态 $x_i(0)$, 攻击信号 $u_{Ki}(t)$ 满足攻击可检测性引理.

证明　由式 (1) 和 (6) 可得第 i 个子系统的误差模型为

$$\begin{aligned} &E_i\dot{e}_i(t) = \\ &(A_i+G_iC_i)e_i(t) + \sum_{j\in N_i^{in}} A_{ij}e_j(t)+ \\ &eq11(B_{Ki} + G_iD_{Ki})u_{Ki}(t), \\ &r_i(t) = C_ie_i(t) + D_{Ki}u_{Ki}(t),\ i \in \{1,2,\cdots,N\}. \end{aligned} \quad (8)$$

假设在初始状态时并未受到攻击信号的影响, 则该电网系统攻击前后对应的状态变量误差值初值为 $e_i(0) = 0$.

充分性. 当误差系统输出为 $r_i(t) = 0$ 时, 系统内存在 K 范围攻击输入 $u_{Ki}(t) \neq 0$. 若初始条件 $x_i(0)$ 与攻击信号 $u_{Ki}(t)$ 具有一致性和非脉冲性, e_i 为第 i 个子区域内状态变量攻击前后对应的误差值的拉普拉斯表示, $\tilde{e}_j$ 为除第 i 个子区域外其他子区域内所有状态变量误差值列排列组成的列向量的拉普拉斯表示, 则满足

$$\begin{bmatrix} sE_i - (A_i + G_iC_i) & -\widetilde{A}_{ij} & -(B_i + G_iD_i) \\ -C_i & 0 & -D_i \end{bmatrix} \times \begin{bmatrix} e_i \\ \widetilde{e}_j \\ g_{Ki} \end{bmatrix} = 0,\ i \in \{1,2,\cdots,N\}. \quad (9)$$

由式 (9) 可知, $C_ie_i = -D_ig_{Ki}$. 代入式 (9) 并化简, 可得到

$$\begin{bmatrix} sE_i - A_i & -\widetilde{A}_{ij} & -B_i \\ -C_i & 0 & -D_i \end{bmatrix} \begin{bmatrix} e_i \\ \widetilde{e}_j \\ g_{Ki} \end{bmatrix} = 0. \tag{10}$$

因 $u_{Ki}(t)$ 为可检测的攻击信号, 与式(10)矛盾, 故 $r_i(t) = 0 \Rightarrow u_{Ki}(t) = 0$.

必要性. 当式(8)表示的误差系统内无攻击信号, 即 $u_{Ki}(t) = 0$ 时, $r_i(t)$ 存在非零值, 满足

$$\begin{bmatrix} sE_i - (A_i + G_iC_i) & -\widetilde{A}_{ij} & -(B_i + G_iD_i) \\ -C_i & 0 & -D_i \end{bmatrix} \times \begin{bmatrix} e_i \\ \widetilde{e}_j \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ r_i \end{bmatrix}, \ i \in \{1, 2, \cdots, N\}. \tag{11}$$

其中 r_i 为 $r_i(t)$ 的拉普拉斯表示. 因为此时式(1)对应的电网系统在 t 时刻未受到攻击信号的影响, 即 $e_i(t) = 0$, 与式(11)矛盾, 所以 $u_{Ki}(t) = 0 \Rightarrow r_i(t) = 0$.

最后证明误差系统在无攻击输入时的稳定性问题. 对于这一大规模的系统, 采用小增益方法将该动态误差系统改写成两个子系统的闭环互联, 即

$$\begin{aligned} &\Gamma_1 : E_i\dot{e}_i(t) = (A_i + G_iC_i)e_i(t) + v(t), \\ &\Gamma_2 : v(t) = \sum_{j \in N_i^{in}} A_{ij}e_j(t). \end{aligned} \tag{12}$$

因为两个子系统均具有因果性和内部稳定性, 所以若该动态误差系统稳定, 则对于任意 $\omega \in R$, 需要满足频谱条件 $\rho(\Gamma_1(j\omega)\Gamma_2) < 1$[12], 如式(7)所示. □

推论 1 设分布式动态状态估计器为

$$\begin{aligned} &E_i\dot{\hat{x}}_i^{(k)}(t) = \\ &(A_i + G_iC_i)\hat{x}_i^{(k)}(t) + \sum_{j \in N_i^{in}} A_{ij}\hat{x}_j^{(k-1)}(t) - G_iy_i(t), \\ &r_i^{(k)}(t) = y_i(t) - C_i\hat{x}_i^{(k)}(t), \ i \in \{1, 2, \cdots, N\}. \end{aligned} \tag{13}$$

当且仅当 $u_{Ki}(t) = 0 (t \in [0, T])$ 时, $\lim\limits_{k \to \infty} \|r^{(k)}(t)\|_\infty = 0$. 需满足 $(E_i, A_i + G_iC_i)$ 为正则且赫尔维茨稳定, 且

$$\rho((j\omega E_i - A_i - G_iC_i)^{-1}\tilde{A}_{ij}) < 1, \ \forall \omega \in R. \tag{14}$$

其中: 已知系统初始状态 $x_i(0)$, 攻击信号 $u_{Ki}(t)$ 满足攻击可检测性引理.

证明 $u_{Ki} = 0 \Leftrightarrow \lim\limits_{k \to \infty} \|r^{(k)}(t)\|_\infty = 0$ 的证明同定理 1. 由高斯-雅克比波形松弛法[13]的收敛性可知, 当且仅当满足推论 1 中两个条件时, $\lim\limits_{k \to \infty} \hat{x}^{(k)}(t) \to \hat{x}(t)$. □

注 1 推论 1 利用高斯-雅克比波形松弛法将连续的交换方式以分段的方式离散化, 解决了定理 1 中需要每个联系的控制中心不断交换本地估计向量的问题, 可以缓解连续数据交换给电网带来的通信压力.

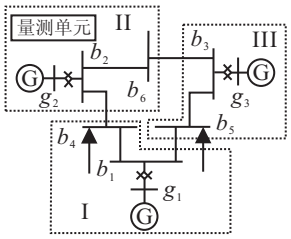
需要说明的是, 对于攻击检测器的部分, 因有可能存在噪声干扰, 给出一个阈值 $\Gamma \in R$, 即当

$$\|r(t)\|_\infty > \Gamma \tag{15}$$

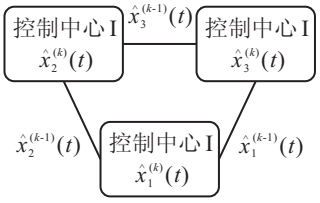
时, 攻击检测器输出 True, 并将信息发送到该区域内的调度控制中心.

4 3 机 9 节点分布式电网系统攻击检测仿真

以分布式 9 总线电网系统为例说明分布式动态状态估计器对于分布式电网中数据攻击检测的有效性, 系统框图如图 2 所示.



(a) 物理结构



(b) 信息结构

图 2 3 机 9 节点分布式电网系统

系统含有 3 个子区域, 分别为 $\{g_1, b_1, b_4\}$、$\{g_2, b_2, b_6\}$ 和 $\{g_3, b_3, b_5\}$. $\{g_2, g_2, g_3\}$ 为 3 个发电机, $\{b_1, b_2, \cdots, b_6\}$ 为 6 个用户负荷端. 每个子区域对应一个控制中心, 箭头方向为各子区域间潮流方向. 假设攻击点位于 b_4、b_5 处, 观测点位于 g_2 处. 以子区域 I 内的控制中心 I 为例, 给出分布式动态状态估计算法如下.

Step 1: 以 $k = 0$ 为初始条件, 令 $k = k + 1$, 控制中心 I 接收由控制中心 II 传送过来的状态估计值 $\hat{x}_2^{(k-1)}(t)$, 并按式(13)更新本区域内的状态估计值 $\hat{x}_1^{(k)}(t)$.

Step 2: 控制中心 I 将上一次迭代(即 $k-1$ 次迭代)后求得的本区域状态估计值 $\hat{x}_2^{(k-1)}(t)$ 传送到控制中心 III 中.

Step 3: 循环至 k 达到设定值.

当 k 足够大时, 迭代结果收敛, 得到最终的状态估计值. 对于本地状态估计器而言, 根据式(14)对系统是否存在攻击信号进行检测, 当且仅当在 $u_K(t) = 0 (t \in [0, T])$ 时, 若 $k \to \infty$, 则 $\|r^{(k)}(t)\|_\infty = 0$. 通过这种分布式的状态估计算法, 不仅可以通过连续时间分段化减小通信层面的压力, 而且可以实现通过各子区域间的通信协作实现对电网复杂结构矩阵的降维, 使得状态估计算法更加具有时效性和稳定性.

在图2所示的3机9节点电网系统中, 攻击输入矩阵 $B_k = [e_8 \ \ e_9]$, $D_K = [0 \ \ 0]$, 量测单元矩阵 $C = [e_2 \ \ e_5]^{\mathrm{T}}$, 系统状态变换矩阵中发电机惯性量矩阵

$$M = blk\mathrm{diag}[M_1 \ \ M_2 \ \ M_3],$$

阻尼系数矩阵

$$D = blk\mathrm{diag}[D_1 \ \ D_2 \ \ D_3];$$

$L_i = \begin{bmatrix} L_{i1} & L_{i2} \\ L_{i3} & L_{i4} \end{bmatrix} \in R^{(n+m)\times(n+m)}$ 和 $L_{ij} = \begin{bmatrix} 0 & L_{ij}^{\prime} \\ 0 & L_{ij}^{\prime\prime} \end{bmatrix} \in R^{(n+m)\times(n+m)}$ 为导纳矩阵或基尔霍夫矩阵, 是图的矩阵的拉普拉斯表示. 这里需要提出的是, 量测点处传感器对应的物理特性参数在状态估计与求差值的过程中并不影响对攻击信号的检测, 故假设 $D_K = [0 \ \ 0]$ 不影响结论的有效性. 在式(1)所示的分布式动态数学模型中, 有

$$E_i = blk\mathrm{diag}[I \ \ M_i \ \ 0],$$

$$A_i = -\begin{bmatrix} 0 & -I & 0 \\ L_{i1} & -D_i & L_{i2} \\ L_{i3} & 0 & L_{i4} \end{bmatrix},$$

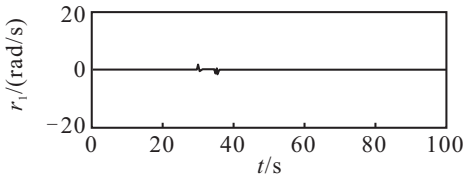
$$A_{ij} = -\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & L_{ij}^{\prime} \\ 0 & 0 & L_{ij}^{\prime\prime} \end{bmatrix}.$$

采用文献[14]的电网参数, 容易得到该系统的分布式动态数学模型.

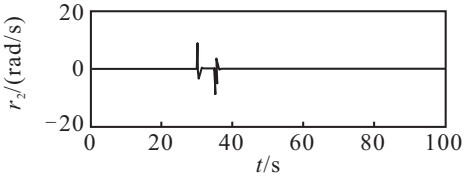
假设在发电机 g_1 处设置量测单元观测输出值, 攻击者在 b_4、b_5 处分别注入满足引理1的一类数据攻击 $u_1(t)$、$u_2(t)$, 系统的攻击效果如图3(a)～图3(c)所示. 当系统内无攻击信号时, 系统处于正常运行的稳定状态, 设为零状态. 当系统运行到 $t = 30$ s时, 注入一定攻击范围的攻击信号 $u_K(t)$, 该攻击信号给电网系统带来了很大的波动, 严重时甚至会使得电网系统脱离稳定运行状态直至崩溃.

对该数据攻击下的分布式9总线电网系统的每个子区域应用分布式动态状态估计器后得到的输出估计差值如图3(d)～图3(f)所示. 可知, 在 $t = 30$ s之前子区域内无攻击信号, 状态估计器输出的状态差值为0; 当 $t = 30$ s时, 受到攻击信号影响的子区域内出现非正常工作状态, 状态估计器迅速通过估计算法得到状态差值并实现跳变, 使攻击检测器能够成功检测到攻击信号, 并据此对电网施加控制信号.

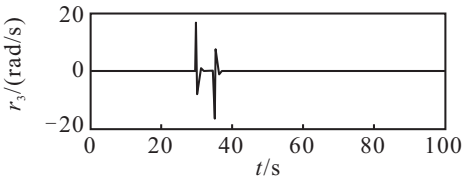
需要说明的是, 若要证明分布式状态估计器中加入的 k 次迭代算法可以得到准确的估计值, 则由 k 次迭代后差值收敛即可证明分布式状态估计器的可行性, 如图4所示. 对于该分布式系统, 在 $k = 20 \sim 25$ 时算法收敛, 若系统进一步复杂化, 迭代次数将增加.



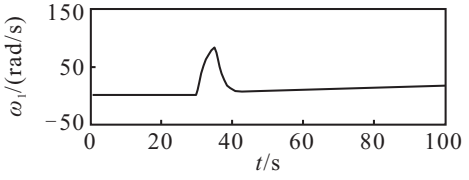
(a) 子区域1状态估计器输出



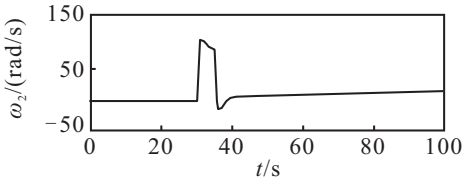
(b) 子区域2状态估计器输出



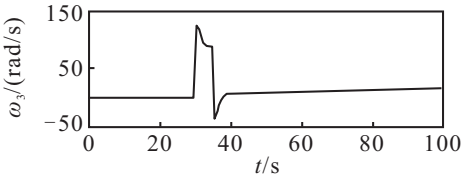
(c) 子区域3状态估计器输出



(d) 数据攻击下子区域1量测单元输出



(e) 数据攻击下子区域2量测单元输出



(f) 数据攻击下子区域3量测单元输出

图 3　存在数据攻击下的电网各子区域内波形

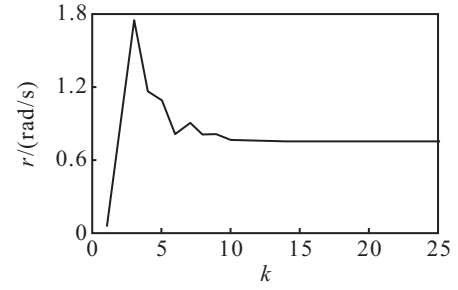


图 4　分布式估计算法 k 次迭代收敛图

5 结 论

本文对数据攻击下的智能电网安全控制进行了研究. 首先根据电力系统线性摆动方程和功率流守恒方程给出分布式动态系统的线性奇异状态空间数学模型表示方法, 并在攻击可检测判据的基础上发展了一种分布式动态状态估计器算法, 通过加入波形松弛迭代法实现连续时间分段化, 最终使得每个子区域的控制中心只需要知道本地结构信息和与相关联子区域之间的估计状态互传, 即可实现对本地信息的估计与更新, 进而达到全局攻击检测的效果. 此外, 在电网系统对于数据攻击检测的整个调度控制过程中, 对于攻击检测器的部分, 为了避免将噪声干扰误以为是攻击信号, 加入阈值限制辅助判断, 以保证对智能电网攻击检测的有效性.

参考文献(References)

[1] 霍司天. 智能输电网信息安全技术研究[D]. 北京: 华北电力大学电气与电子工程学院, 2011.
(Huo S T. Security technology research of smart transmission grid[D]. Beijing: Department of Electrical and Electronic Engineering, North China Electric Power University, 2011.)

[2] 李碧君, 薛禹胜, 顾锦汶, 等. 基于快速分解正交变换状态估计算法的坏数据检测与辨识[J]. 电力系统自动化, 1999, 23(20): 1-5.
(Li B J, Xue Y S, Gu J W, et al. Bad data detection and identification based on a state estimation algorithm with fast decomposition orthogonal transformation[J]. Automation of Electric Power System, 1999, 23(20): 1-5.)

[3] 蔡昌春, 丁晓群, 王斌. 基于改进最小二乘法的电力系统状态估计[J]. 浙江电力, 2006(4): 6-10.
(Cai C C, Ding X Q, Wang B. State estimation of power system based on improved least-squares algorithm[J]. Zhejiang Electric Power, 2006(4): 6-10.)

[4] 倪小平, 张步涵. 基于等效电流量测变换的状态估计及不良数据检测与辨识方法[J]. 电网技术, 2002, 26(8): 12-15.
(Ni X P, Zhang B H. A state estimation method for bad data detection and identification based on equivalent current measurement transformation[J]. Power System Technology, 2002, 26(8): 12-15.)

[5] 华国栋, 应剑烈, 刘耀年. 基于分布式抗差最小二乘法的状态估计[J]. 东北电力大学学报: 自然科学版, 2008, 28(1): 60-67.
(Hua G D, Ying J L, Liu Y N. State estimation based on distributed robust least square method[J]. J of Northeast Dianli University: Natural Science Edition, 2008, 28(1): 60-67.)

[6] 马静, 孙书利. 广义系统信息融合稳态与自校正满阶Kalman滤波器[J]. 控制理论与应用, 2011, 28(9): 1169-1174.
(Ma J, Sun S L. Information fusion steady-state and self-tuning full-order Kalmanfilters for descriptor systems[J]. Control Theory & Applications, 2011, 28(9): 1169-1174.)

[7] 张海波, 易文飞. 基于异步迭代模式的电力系统分布式状态估计方法[J]. 电力系统自动化, 2014, 38(9): 125-132.
(Zhang H B, Yi W F. Distributed state estimation of power system based on asynchronous iteration mode[J]. Automation of Electric Power System, 2014, 38(9): 125-132.)

[8] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids[J]. ACM Trans on Information and System Security, 2011, 14(1): 13.

[9] Asada E N, Garcia A V, Romero R. Identifying multiple interacting bad data in power system state estimation[C]. Power Engineering Society General Meeting. San Francisco: IEEE, 2005: 571-577.

[10] Pasqualetti F, Dorfler F, Bullo F. Cyber-physical attacks in power networks: Models, fundanmental limitations and monitor design[C]. Proc of IEEE Conf Decision Control and Eur. Orlando, 2011: 2195-2201.

[11] Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems[J]. IEEE Trans on Automatic Control, 2013, 58(11): 2715-2729.

[12] Skogestad S, Postlethwaite I. Multivariable feedback control analysis and design[C]. 2nd ed. New York: Wiley, 2005: 55-64.

[13] Smith R S. A decoupled feedback structure for covertly appropriating networked control systems[J]. World Congress, 2011, 18(1): 90-95.

[14] Scholtz E. Observer-based monitors and distributed wave controllers for electromechanical disturbances in power systems[D]. Boston: Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 2004.

(责任编辑: 郑晓蕾)