受攻击信息物理系统的分布式安全状态估计与控制 — 一种有限时间方法

敖 伟 [1] 宋永端 [2, 3] 温长云 [4]

摘 要 研究具有非线性耦合特性信息物理系统 (Cyber physical systems, CPS) 在被攻击情况下的分布式有限时间状态安全估计和控制问题. 首先, 提出一种由分布式安全测量预选器和有限时间观测器组成的分布式有限时间状态安全估计策略, 可确保系统的状态在预设的有限时间之内被准确估计出来. 然后, 利用获得的安全状态估计, 借助反步设计方法, 建立一套分布式有限时间安全控制算法. 理论分析表明, 该方法可以保证系统能在有限时间内实现对给定信号的跟踪. 最后, 通过微电网系统仿真验证了所提方法的有效性.

关键词 受攻击信息物理系统, 分布式状态安全估计, 分布式安全控制, 有限时间方法

引用格式 敖伟, 宋永端, 温长云. 受攻击信息物理系统的分布式安全状态估计与控制 — 一种有限时间方法. 自动化学报, 2019, **45**(1): 174−184

DOI 10.16383/j.aas.c180385

Distributed Secure State Estimation and Control for CPSs Under Sensor Attacks — A Finite Time Approach

AO Wei[1] SONG Yong-Duan[2, 3] WEN Chang-Yun[4]

Abstract This paper investigates the problem of distributed secure state estimation and control for nonlinearly coupled interconnected cyber physical systems (CPS) under sensor attacks. Distributed schemes consisting of pre-selectors and observers are presented to solve the secure state estimation problem. Then, with the obtained state estimation and following the backstepping design procedure, distributed secure control algorithms are derived. Theoretical analysis shows that, with the proposed distributed secure observers and controllers, not only the state estimation of the CPS under attacks is obtained in a given finite time, but also the state tracking is ensured in a finite time. Finally, the developed algorithms are applied to an islanded micro-grid system as an illustration, verifying the effectiveness of the proposed method.

Key words Cyber physical system (CPS) under attacks, distributed secure state estimation, distributed secure control, a finite time approach

Citation Ao Wei, Song Yong-Duan, Wen Chang-Yun. Distributed secure state estimation and control for CPSs under sensor attacks — a finite time approach. *Acta Automatica Sinica*, 2019, **45**(1): 174−184

随着信息技术的广泛应用, 信息物理系统 (Cyber physical systems, CPS) (交通系统、智能电网系统以及高速铁路系统), 以其物理动态过程与信息传输处理过程的紧密耦合[1], 成为近期研究热点. 不过, 正是由于信息处理与动态过程的紧密关联, 使其特别容易受到数据传输中的错误或攻击影响, 进而造成损失或重大破坏, 比如巴西电网大停电事故[2]以及针对伊朗的震荡波病毒攻击[3].

当前已有一些文章涉及信息物理系统安全问题, 其中大体包含两类. 第一类着重研究攻击检测问题. 比如, 文献 [4] 研究信息物理系统的攻击检测与识别问题, 从系统理论和图论的角度刻画监测系统的固有缺陷, 并设计一种基于 Luenberger 观测器的监测器, 用于攻击检测和识别, 但是其只能实现渐近收敛, 故检测时间可能非常长. 文献 [5] 提出一种基于

收稿日期 2018-05-31 录用日期 2018-08-14
Manuscript received May 31, 2018; accepted August 14, 2018
国家自然科学基金 (61773081, 61860206008), 重庆高校优秀成果转化项目 (KJZH17102) 资助
Supported by National Natural Science Foundation of China (61773081, 61860206008), and the Technology Transformation Program of Chongqing Higher Education University (KJZH17102)
本文责任编委 刘向杰
Recommended by Associate Editor LIU Xiang-Jie
1. 重庆科技学院数理与大数据学院 重庆 401331 中国 2. 重庆大学信息物理社会可信服务计算教育部重点实验室 重庆 400044 中国 3. 重庆大学自动化学院 重庆 400044 中国 4. 南洋理工大学电气工程与电子学院 新加坡 639798 新加坡
1. College of Mathematics and Science, the Chongqing University of Science and Technology, Chongqing 401331, China 2. Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing 400044, China 3. School of the Automation, Chongqing University, Chongqing 400044, China 4. School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798, Singapore

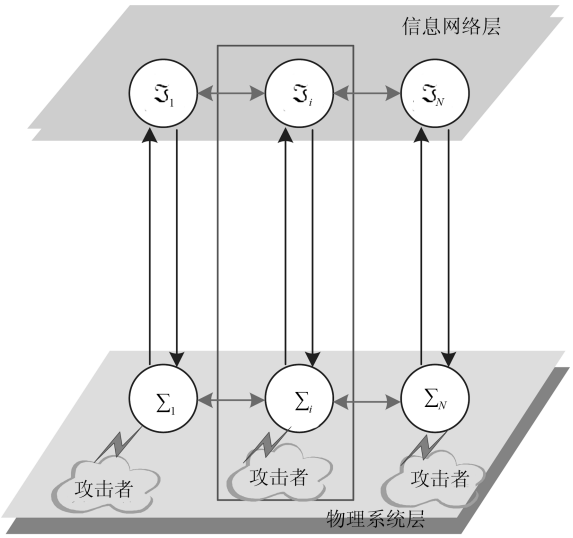
滑模观测器的方法, 可分别对信息物理系统中存在的状态攻击和输出攻击进行检测和重构, 但该方法需要满足所谓的观测器匹配条件. 文献 [6] 通过研究系统的强观测性, 并利用系统动态特征向量, 提出一种攻击可检测的充分必要条件. 不过, 他们都没有涉及状态安全估计与控制问题. 第二类主要关注状态安全估计和安全控制器设计. 比如, 文献 [7] 针对部分传感器受到攻击的信息物理系统, 提出一种便于计算的解码算法, 用以估计系统状态, 并刻画该算法能够容许的最大受攻击传感器数量的上界; 进而, 这些结果在文献 [8] 中得到了扩充, 该文即不仅展示了通过设计局部安全控制器可以提升系统面对攻击的性能, 同时还提出一种基于 L_1/L_r 的编码器实现状态的安全估计. 此外, 通过研究系统的稀疏观测性, 文献 [9] 指出, $2s$-稀疏可观测, 那当且仅当其受到不超过 s-稀疏攻击时, 状态可以被安全估计出来; 文献 [10] 拓展这一结论, 并利用高效满足性模态理论, 设计一种新型的多模态 Luenberger 观测器, 对安全估计问题的复杂性进行了优化. 不过, 文献 [7−10] 中的安全估计算法都是集中式的, 且其估计误差为指数衰减, 这使得估计结果可能要较长时间才能满足实际需求. 此外, 我们在文献 [11] 中, 针对受到攻击的线性信息物理系统, 提出一种基于有限时间观测器的安全估计算法, 可以确保在预设有限时间完成状态安全估计, 不过, 该方法仍然是集中式的, 同时也没有涉及安全控制问题. 进而, 文献 [12] 进一步拓展这些结果, 提出一种分布式的状态安全估计与安全控制策略; 不过, 其研究的信息物理系统之间仅含有线性耦合, 且其安全控制方法依赖分数阶动态面技术, 只能保证动态面在有限时间内达到, 并不能确保期望状态误差在有限时间内收敛到零. 而实际的信息物理系统, 比如智能电网系统, 其分布式特点比较明显, 且其子系统之间的耦合也可能是非线性的; 同时为应对恶意攻击, 需要在有限时间内将跟踪误差控制到零. 因此, 这就需要探索新的有限时间分布式安全估计以及安全控制设计方法.

正是基于上述考虑, 本文针对一类受到攻击的由多个子系统组成的非线性耦合信息物理系统, 研究其分布式安全估计以及分布式安全控制问题. 相关的系统结构及提出的方法和策略如图 1 所示. 本文的主要贡献包括:

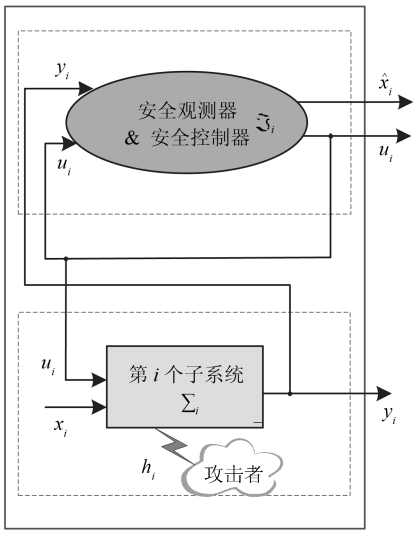
1) 针对一类含有非线性耦合的信息物理系统, 提出一种由安全测量预选器和有限时间观测器组成的分布式有限时间状态安全估计策略. 当满足一定条件时, 该策略可确保系统状态在预设有限时间之内被准确估计出来;

2) 利用获得的安全状态估计, 采用反步设计方法建立分布式有限时间安全控制律;

3) 基于李亚普洛夫稳定性理论, 严格论证该控制律可以保证系统在有限时间内跟踪期望信号, 且各系统状态, 观测器信号以及控制信号有界. 该方法的有效性也通过仿真实验得到验证.



(a) 相互耦合的分布式信息网络系统
(a) Block diagram of interconnected CPS



(b) 第 i 个子系统的安全状态估计器与控制器
(b) Secure observer and controller for the i-th subsystem

图 1　受到传感器攻击的信息物理系统与有限时间状态安全估计与控制框图

Fig. 1　The diagram of the CPS under sensor attacks and the finite time secure state estimation and control

本文后续内容由以下几部分组成: 第 1 节介绍研究对象模型并提出研究目的; 第 2 节提出一种由安全预选器和有限时间观测器组成的状态估计策略, 解决分布式安全状态估计问题; 第 3 节提出一种分布式控制算法, 解决分布式安全控制问题; 第 4 节将

提出的方法在微电网中仿真实验, 验证该方法的有效性; 第 5 节对本文做总结.

1 系统模型

本文考虑由 N 个相互耦合子系统组成的信息物理系统, 其结构见图 1 (a). 由于物理特性, 子系统相互之间具有一定的非线性动态耦合; 相应地, 为完成控制、监测功能, 子系统之间还包含信息处理系统即通过计算机处理和信息网络设施, 将测量、控制信号传输到监测或控制系统; 而这些信息处理与传输过程, 有可能遭受恶意攻击. 基于这些考虑, 该信息物理系统中的第 i 个受到攻击的子系统, 可用下述模型描述.

$$\begin{cases} \dot{x}_{i,1}(t) = a_{i,1}x_{i,1}(t) + x_{i,2}(t) \\ \qquad\qquad \vdots \\ \dot{x}_{i,n-1}(t) = a_{i,n-1}x_{i,1}(t) + x_{i,n}(t) \\ \dot{x}_{i,n}(t) = a_{i,n}x_{i,1}(t) + b_iu_i(t) + f_i(\bar{\boldsymbol{x}}, t) \\ \boldsymbol{y}_i(t) = C_i\boldsymbol{x}_i(t) + \boldsymbol{\eta}_i(t) \end{cases} \tag{1}$$

其中, $\boldsymbol{x}_i(t) = [x_{i,1}(t), \cdots, x_{i,n}(t)]^{\mathrm{T}} \in \mathbf{R}^n$ 为系统的未知状态, $u_i(t) \in \mathbf{R}$ 为受控输入信号; $\boldsymbol{y}_i(t) \in \mathbf{R}^{p_i}$ 是经传输得到的测量信号, 需注意, 由于存在恶意攻击者, $\boldsymbol{y}_i(t)$ 可能被任意篡改, $\boldsymbol{\eta}_i(t) \in \mathbf{R}^{p_i}$ 即为攻击者注入的恶意攻击信号; $C_i = [C_{i,0}, \cdots, C_{i,0}]^{\mathrm{T}} \in \mathbf{R}^{p_i \times n}$ 为系统测量矩阵, 其中 $C_{i,0}^{\mathrm{T}} = [1, 0, \cdots, 0]^{\mathrm{T}} \in \mathbf{R}^n$; 而 $f_i(\bar{\boldsymbol{x}}, t)$ 代表第 i 个子系统受到其他所有子系统的非线性耦合效应, $\bar{\boldsymbol{x}} = [x_{1,1}, \cdots, x_{N,1}]^{\mathrm{T}}$ 表示所有子系统状态第一个分量组成的向量.

注 1. 文献 [12] 仅考虑存在纯线性耦合的情况, 这局限了其应用范围; 而本文研究的系统模型包含非线性耦合分量, 这样可能更符合实际情况使其适用范围更广. 另外, 文献 [12] 设计的控制律是基于分数阶动态面的, 并不能保证受控状态在有限时间内跟踪上期望信号. 因此, 需要探索新的方法实现对状态的有限时间跟踪控制.

正如文献 [4] 所述, 许多实际信息物理系统, 譬如智能电网、高铁系统[13] 等, 都可用形如式 (1) 的模型描述. 此外, 随着信息技术的发展, 在实际的系统[14−15] 中, 经常利用多路传感器采集同一信号, 以便提高系统中信号测量的可靠性、冗余性与安全性. 鉴于此, 本文也采用该方法. 因此, 输出分布矩阵即 C_i, 便如模型 1 中所示.

本文假定, 对于第 i 个子系统, p_i 路传感器中仅有 s_i 路是可被攻击者任意操纵的. 除此之外, 本文不对攻击者具有的关于系统的信息和操纵信号的能力作任何限制. 此外, 受安全检测与估计方面[4, 8] 等文献的启发, 为了刻画安全估计可实现的充分条件, 本文引入如下定义.

定义 1. s-稀疏攻击[8]: 给定攻击向量 $\boldsymbol{\eta}_i(t)$, 如果存在集合 $\Lambda_i \subset \{1, \cdots, p_i\}$ 且 $Card(\Lambda_i) = p_i - s$, 对任意 $s \in \mathbf{N}$ 和 t, 有 $\eta_{i,j}(t) = 0$, 而 $\eta_i(t)$ 的其他 s 个分量不一定为零, 则称它是一个 s-稀疏攻击, 或它是一个稀疏指数为 s 的攻击向量. s 即为攻击向量的稀疏指数.

注 2. 定义 1 主要用于刻画如 (1) 所示受攻击信息物理系统, 其状态安全估计可解的充分条件, 见第 3.1 节.

2 问题描述

本文的主要目标是解决如下两个问题.

1) 分布式有限时间安全状态估计问题: 即针对如式 (1) 所示受攻击信息物理系统, 提出其分布式状态安全估计可解的充分条件, 并设计安全估计器, 在有限时间内获得系统的真实状态.

2) 分布式有限时间安全问题: 即针对如式 (1) 所示受攻击信息物理系统, 在安全状态估计实现的基础上, 设计分布式安全控制器, 使系统能够在有限时间内跟踪任意给定信号.

3 分布式有限时间状态安全估计

本节将提出一种由安全预选器与有限时间观测器构成的分布式有限时间状态安全估计策略.

3.1 安全测量预选器设计

首先, 受文献 [12] 启发, 利用定义 1, 对于分布式信息物理系统 (1), 可给出其状态可安全估计的充分条件.

条件 1. 对于受到稀疏攻击的分布式信息物理系统 (1), 其中第 i 个子系统中的稀疏指数为 s_i, s_i 满足如下条件:

$$s_i \leq \begin{cases} \dfrac{1}{2}(p_i - 1), & p_i \text{ 为奇数} \\ \dfrac{1}{2}p_i - 1, & p_i \text{ 为偶数} \end{cases} \tag{2}$$

命题 1. 对于受到稀疏攻击的分布式信息物理系统 (1), 其中第 i 个子系统中的稀疏指数为 s_i, 若条件 1 成立, 那其状态安全估计是可实现的.

证明. 命题 1 的证明与文献 [12] 中相似, 故在此省略. □

注 3. 对于集中式信息物理系统模型, 受攻击时状态安全估计的可实现条件在文献 [7−11] 中给出; 而命题 1 则进一步将对象扩展到受攻击的分布式信息物理系统, 并提出了状态可被安全估计得到的充分条件. 此外, 需要注意, 命题 1 虽然刻画了受

攻击地信息物理中的状态可安全估计的充分条件, 但由于系统 1 含有非线性耦合特性, 文献 [12] 中设计的安全观测器并不能直接应用, 所以具体的状态估计方法特别是有限时间估计方法还需要精巧地设计.

基于条件 1, 同时受文献 [12] 启发, 可以设计一种分布式策略, 检索出每个系统中未受攻击的传感数据. 在此, 先介绍一种中间值求取算子: 给定向量 $y_i(t)$, 将其元素按大小排序得到一个新的向量 $\boldsymbol{v}_i = [v_{i,1}, \cdots, v_{i,p_i}]^{\mathrm{T}}$, 其中 $v_{i,1} \leq \cdots \leq v_{i,p_i}$. 那么, 对于向量 $y_i(t)$ 的中间值算子如下:

$$Med\left[\boldsymbol{y}_i(t)\right] = \begin{cases} v_{i,in}, & p_i\text{为奇数} \\ \dfrac{1}{2}(v_{i,in} + v_{i,in+1}), & p_i\text{为偶数} \end{cases} \tag{3}$$

其中, p_i 为偶数时, $in = \frac{1}{2}p_i$; 而 p_i 为奇数时, $in = \frac{1}{2}(p_i + 1)$. 当条件 1 成立时, 针对第 i 个子系统的分布式安全测量预选器设计如下:

$$z_{p,i}(t) = Med\left[y_i(t)\right] \tag{4}$$

关于上述预选器, 下述结论成立.

引理 1. 对于含有攻击的信息物理系统 (1), 当条件 1 成立时, 利用安全测量预选器 (4), 对所有时刻, 下式成立.

$$x_{i,1}(t) = z_{p,i}(t) \tag{5}$$

证明. 引理 1 的证明与文献 [12] 中相似, 故省略. □

注 4. 值得注意的是, s_i 为攻击向量中非零信号的数目, 即受到攻击的传感器的数量; r_i 为不受攻击的传感器的数量; 而 q_i 表示不受攻击的传感器超过受攻击的传感器的数量. 实际上, 这部分分析表明, 只要不受攻击的传感器超过受攻击的传感器的数量, 即 $q_i > 0$, 那么利用排序方法和中间值算子, 都能将 "中间" 不受攻击的信号提取出来. 需要指出的是, 由于预选器 (4) 主要通过分析多路传输信号的差异, 从而提取出 "安全" (未受攻击) 的测量信号; 此外, 多路传感器采集的是同样的信号, 而实际信息系统内部的非线性特性在输出通道的表现都是相同的, 所以, 该预选器可以应对系统中含有非线性耦合的情况.

3.2　分布式状态安全估计器设计

受文献 [16] 中集中式有限时间观测器以及文献 [12] 中分布式有限时间安全状态估计器启发, 利用式 (4) 所设计的预选器, 对于受到攻击的信息物理系统 (1) 中第 i 个子系统, 可设计如下分布式安全状态估计器.

$$\begin{cases} \dot{\hat{\boldsymbol{\zeta}}}_i(t) = \bar{F}_i\hat{\boldsymbol{\zeta}}_i(t) + \bar{H}_i\bar{\boldsymbol{f}}_i(t) + \bar{L}_i z_{p,i}(t) + \\ \qquad\quad \bar{H}_i B_i u_i(t) \\ \hat{\boldsymbol{x}}_i(t) = \bar{M}_i[\hat{\boldsymbol{\zeta}}_i(t) - e^{\bar{F}_i T_{e,i}}\hat{\boldsymbol{\zeta}}_i(t - T_{e,i})] \end{cases} \tag{6}$$

其中, $\hat{\boldsymbol{\zeta}}_i(t) \in \mathbf{R}^{2n}$ 为观测器状态, 而 $\hat{\boldsymbol{x}}_i(t)$ 作为观测器输出是对真实状态的安全估计, $\bar{\boldsymbol{f}}_i(t) = [0, \cdots, 0, f_i(\bar{x}, t)]^{\mathrm{T}}$, $\bar{H}_i = \begin{bmatrix} I_{n\times n} \\ I_{n\times n} \end{bmatrix}$, $\bar{F}_i = \begin{bmatrix} F_{i,1} & 0 \\ 0 & F_{i,2} \end{bmatrix}$, $\bar{L}_i = \begin{bmatrix} L_{i,1} \\ L_{i,2} \end{bmatrix}$, $F_{i,j} = A_{i,0} - L_{i,j}C_i$ 为严格稳定矩阵, $A_{i,0} = \begin{bmatrix} a_{i,1} & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ a_{i,n-1} & 0 & \cdots & 1 \\ a_{i,n} & 0 & \cdots & 0 \end{bmatrix}$, $j = 1, 2$. $T_{e,i}$ 为一常数, 其选择满足如下不等式.

$$\det\begin{bmatrix} \bar{H}_i & \bar{F}_i^{T_{e,i}}\bar{H}_i \end{bmatrix} \neq 0 \tag{7}$$

为方便起见, 将所有子系统的 $T_{e,i}$ 取为相同值, 即 $T_{e,i} = T_e$, $i = 1, \cdots, N$.

此外, 矩阵 $\bar{M}_i$ 的计算方式如下:

$$\bar{M}_i = \begin{bmatrix} I_{n\times n} & \mathbf{0}_{n\times n} \end{bmatrix}\begin{bmatrix} \bar{H}_i & \bar{F}_i^{T_e}\bar{H}_i \end{bmatrix}^{-1} \tag{8}$$

注 5. 虽然分布式有限时间观测器 (6) 是受文献 [12] 中方法启发而来, 且形式上有一定的相似之处, 但由于非线性耦合效应 $f_i(\bar{\boldsymbol{x}}_i, t)$ 的存在, 使该文结果并不能直接应用到系统 (1) 中. 因此, 本文利用 $H_i\bar{\boldsymbol{f}}_i(t)$ 项对信息物理系统中的非线性耦合部分进行补偿, 才能确保有限时间安全状态估计的实现.

利用上述提出的预选器与有限时间观测器, 能够确保在条件 1 满足时, 在有限时间内解决状态安全估计问题, 即可表述为如下定理.

定理 1. 针对含有攻击的信息物理系统 (1), 分布式输出预选器 (4) 和分布式有限时间观测器 (6). 当条件 1 成立且 T_e 和 $\bar{M}_i$ 分别满足 (7) 和 (8) 时, 信息物理系统 (1) 中的状态, 可以在预设的有限时间内准确地得到, 即当 $t \geq T_e$ 时,

$$\boldsymbol{x}_i(t) = \hat{\boldsymbol{x}}_i(t) \tag{9}$$

证明. 记估计误差为: $\bar{\boldsymbol{e}}_{\zeta,i}(t) = H\boldsymbol{x}_i(t) - \hat{\bar{\boldsymbol{\zeta}}}_i(t)$, 由于预选器 (4) 可以得到未受攻击测量信号, 那么估计误差的动态特性如下:

$$\dot{\bar{\boldsymbol{e}}}_{\zeta,i}(t) = \bar{H}_i\boldsymbol{x}_i(t) - \dot{\hat{\bar{\boldsymbol{\zeta}}}}_i = \bar{F}_i\bar{\boldsymbol{e}}_{\zeta,i}(t) \tag{10}$$

显然, 若将初始误差记为 $\bar{\boldsymbol{e}}_{\zeta,i}(0)$, 那么误差 $\bar{\boldsymbol{e}}_{\zeta,i}(t)$ 的特性可以刻画如下.

$$\bar{\boldsymbol{e}}_{\zeta,i}(t)=e^{\bar{F}_i t}\bar{\boldsymbol{e}}_{\zeta,i}(0)=\mathrm{e}^{\bar{F}_i T_e}\bar{\boldsymbol{e}}_{\zeta,i}(t-T_e) \tag{11}$$

注意到 $\bar{\boldsymbol{e}}_{\zeta,i}(t)=\bar{H}_i\boldsymbol{x}_i(t)-\hat{\bar{\boldsymbol{\zeta}}}_i(t)$ 以及 $\bar{\boldsymbol{e}}_{\zeta,i}(t-T_e)=\bar{H}_i\boldsymbol{x}_i(t-T_e)-\hat{\bar{\boldsymbol{\zeta}}}_i(t-T_e)$, 那么根据式 (11) 可得:

$$\bar{H}_i\boldsymbol{x}_i(t)-\mathrm{e}^{\bar{F}_i T_e}\bar{H}_i\boldsymbol{x}_i(t-T_e)=\hat{\bar{\boldsymbol{\zeta}}}_i(t)-\mathrm{e}^{\bar{F}_i T_e}\hat{\bar{\boldsymbol{\zeta}}}_i(t-T_e) \tag{12}$$

由于 T_e 为满足式 (7) 的常数, 那么根据式 (8), 可得:

$$\bar{M}_i\begin{bmatrix}\bar{H}_i & \mathrm{e}^{\bar{F}_i T_e}\bar{H}_i\end{bmatrix}=\begin{bmatrix}I_{n\times n} & 0_{n\times n}\end{bmatrix} \tag{13}$$

利用式 (13), 在式 (12) 两侧同时左乘以 $\bar{\boldsymbol{M}}_i$, 可得:

$$\boldsymbol{x}_i(t)=\bar{M}_i[\hat{\bar{\boldsymbol{\zeta}}}_i(t)-\mathrm{e}^{\bar{F}_i T_e}\hat{\bar{\boldsymbol{\zeta}}}_i(t-T_e)] \tag{14}$$

显然, 比较式 (14) 与式 (6), 即可得到, 当 $t\geq T_e$ 时, 式 (9) 成立. □

4 分布式有限时间安全控制器设计

受文献 [17] 启发, 本节提出一种基于反步法的分布式有限时间安全控制器, 使得受到攻击的信息物理系统 (1) 依然能够在有限时间内跟踪上任意的期望轨迹, 即 $x_{i,1}(t)\to x_{i,d}(t)$, $i=1,\cdots,N$.

4.1 反步法分布式状态安全估计器设计

首先, 定义跟踪误差为 $e_{i,1}(t)=x_{i,1}(t)-x_{i,d}(t)$ 以及 $e_{i,j+1}(t)=\dot{e}_{i,j}(t)$, 则其动态方程如下:

$$\begin{cases}\dot{e}_{i,j}=e_{i,j+1}\\ \dot{e}_{i,n}=\sum\limits_{j=1}^{n}\vartheta_{i,n,j}x_{i,j}+b_i u+f_i-x_{i,d}^{(n)}\end{cases} \tag{15}$$

其中, $f_i=f_i(\bar{\boldsymbol{x}},t)$, $x_{i,d}^{(j)}(t)$ 为 $x_{i,d}(t)$ 的第 j 阶导数; 通过迭代计算可得 $e_{i,k+1}(t)=\sum\limits_{j=1}^{k+1}\vartheta_{i,k,j}x_{i,j}(t)-x_{i,d}^{(k)}(t)$, $k=1,\cdots,i-1$, $j=1,\cdots,n-1$ 和 $i=1,\cdots,n$; 而 $\vartheta_{i,k,j}$ 为迭代计算得到的参数, 其形式如下:

$$\vartheta_{i,k,j}=\begin{cases}\sum\limits_{l=1}^{k}a_{i,l}\vartheta_{i,k-1,l}, & j=1\\ \vartheta_{i,k-1,j-1}, & j\geq 2\end{cases} \tag{16}$$

其中, $\vartheta_{i,1,1}=a_{i,1}$ 和 $\vartheta_{i,1,2}=1$.

下面将采用反步法, 对第 i 个子系统, 设计分布式安全控制器, 使得 $e_{i,1}(t)$ 收敛到 0.

步骤 1. 构造 Lyapunov 函数 $V_{i,1}(t)=\int_0^{e_{i,1}}(s^{\frac{1}{r_1}}-0)^{2-r_2}\mathrm{d}s$, 选择虚拟控制律:

$$\alpha_{i,1}(t)=-\beta_{i,1}\xi_{i,1}^{r_2}(t)+\dot{x}_{i,d}(t) \tag{17}$$

其中, $\xi_{i,1}(t)=e_{i,1}^{\frac{1}{r_1}}(t)$, $r_1=1$, $r_2=r_1-\tau$, $\tau=\frac{\hbar_1}{\hbar_2}$ 而 $\hbar_1$ 为一偶数, $\hbar_2$ 为一奇数, 且 $0<\tau<\frac{1}{n+1}$, $\beta_{i,1}\geq n$. 那么, 计算 $V_{i,1}(t)$ 的导数, 可得:

$$\begin{aligned}\dot{V}_{i,1}(t)=&-\xi_{i,1}^{2-r_2}(\beta_{i,1}\xi_{i,1}^{r_2})+\xi_{i,1}^{2-r_2}(e_{i,2}-\alpha_{i,1})\leq\\ &\xi_{i,1}^{2-r_2}(e_{i,2}-\alpha_{i,1})-n\xi_{i,1}^{2}\end{aligned} \tag{18}$$

步骤 2. 构造 Lyapunov 函数 $V_{i,2}(t)=V_{i,1}(t)+\int_{\alpha_{i,1}}^{e_{i,2}}[s^{\frac{1}{r_2}}-(\alpha_{i,1})^{\frac{1}{r_2}}]^{2-r_3}\mathrm{d}s$, 选择虚拟控制律:

$$\alpha_{i,2}(t)=-\beta_{i,2}\xi_{i,2}^{r_3}(t)+\ddot{x}_{i,d}(t) \tag{19}$$

其中, $\xi_{i,2}(t)=[e_{i,2}(t)]^{\frac{1}{r_2}}-[\alpha_{i,1}(t)]^{\frac{1}{r_2}}$, $\beta_{i,2}$ 为适当的常数. 那么, 求取 $V_{i,2}(t)$ 的导数为

$$\dot{V}_{i,2}(t)\leq-n\xi_{i,1}^{2}+\xi_{i,1}^{2-r_2}(e_{i,2}-\alpha_{i,1})+\xi_{i,2}^{2-r_2+\tau}(e_{i,3}) \tag{20}$$

注意, 根据杨氏不等式, 可得:

$$\begin{aligned}|e_{i,2}-\alpha_{i,1}|\leq&\,2^{2-r_2}\left|(e_{i,2})^{\frac{1}{r_2}}-(\alpha_{i,1})^{\frac{1}{r_2}}\right|^{r_2}=\\ &2^{2-r_2}\xi_{i,2}^{r_2}\end{aligned} \tag{21}$$

进而, 根据式 (21) 可得:

$$\xi_{i,1}^{2-r_2}(e_{i,2}-\alpha_{i,1})\leq\frac{1}{2}\xi_{i,1}^{2}+c_{i,2}\xi_{i,2}^{2} \tag{22}$$

其中, $c_{i,2}$ 为一正常数.

选择 $\beta_{i,2}\geq c_{i,2}+n-1$, 并将式 (19) 代入式 (20), 可得:

$$\begin{aligned}\dot{V}_{i,2}(t)\leq&-n\xi_{i,1}^{2}+\frac{1}{2}\xi_{i,1}^{2}+c_{i,2}\xi_{i,2}^{2}-\beta_{i,2}\xi_{i,2}^{2}+\\ &\xi_{i,2}^{2-r_3}(e_{i,3}-\alpha_{i,2})\leq\xi_{i,2}^{2-r_3}(e_{i,3}-\alpha_{i,2})-\\ &(n-1)(\xi_{i,1}^{2}+\xi_{i,2}^{2})\end{aligned} \tag{23}$$

步骤 3. 假设 $\dot{V}_{i,j-1}(t)\leq-(n-j+2)(\xi_{i,1}^{2}+\cdots+\xi_{i,j-1}^{2})+\xi_{i,j-1}^{2-r_j}(e_{i,j}-\alpha_{i,j-1})$, 那构造 Lyapunov 函数 $V_{i,j}(t)=V_{i,j-1}(t)+\int_{\alpha_{i,j-1}}^{e_{i,j}}[s^{\frac{1}{r_j}}-(\alpha_{i,j-1})^{\frac{1}{r_j}}]^{2-r_j+\tau}\mathrm{d}s$, 选择虚拟控制律:

$$\alpha_{i,j}(t)=-\beta_{i,j}\xi_{i,j}^{r_{j+1}}(t) \tag{24}$$

其中, $\xi_{i,j}=(e_{i,j})^{\frac{1}{r_j}}-(\alpha_{i,j-1})^{\frac{1}{r_j}}$, $r_{j+1}=r_j-\tau$.$V_{i,j}(t)$ 的导数可计算如下:

$$\begin{aligned}\dot{V}_{i,j}(t)\leq&-(n-j+2)(\xi_{i,1}^{2}+\cdots+\xi_{i,j-1}^{2})+\\ &\xi_{i,j-1}^{2-r_j}(e_{i,j}-\alpha_{i,j-1})+\xi_{i,j}^{2-r_{j+1}}e_{i,j+1}\end{aligned} \tag{25}$$

相似地, 根据杨氏不等式, 可得:

$$\xi_{i,j-1}^{2-r_j}(x_{i,j}-\alpha_{i,j-1}) \le 2^{1-r_{j-1}-\tau}|\xi_{i,j-1}|^{2-r_{j-1}-\tau}.$$
$$|\xi_{i,j}|^{r_j} \le \frac{1}{2}\xi_{i,j-1}^2 + c_{i,j}\xi_{i,j}^2 \tag{26}$$

其中, $c_{i,j}$ 为一正常数.

选择 $\beta_{i,j} \ge c_{i,j}+n-j+1$, 并将式 (24) 和式 (26) 代入式 (25), 可得:

$$\dot{V}_{i,j}(t) \le -(n-j+1)(\xi_{i,1}^2+\cdots+\xi_{i,j}^2)+ \xi_{i,j}^{2-r_{j+1}}(e_{i,j+1}-\alpha_{i,j}) \tag{27}$$

步骤 4. 第 n 步. 设计虚拟控制律:

$$\alpha_{i,n}(t) = -\beta_{i,n}\xi_{i,n}^{r_{n+1}}(t) - f_i(\bar{x},t) - \sum_{j=1}^{n}\vartheta_{i,n,j}x_{i,j}(t) + x_{i,d}^{(n)}(t) \tag{28}$$

其中, $\xi_{i,n}(t) = [e_{i,n}(t)]^{\frac{1}{r_n}} - [\alpha_{i,n-1}(t)]^{\frac{1}{r_n}}$, $r_{n+1} = r_n - \tau$, $\beta_{i,n} \ge c_{i,n}+1$ 而 $c_{i,n}$ 为一正常数. 那么, 设计第 i 个子系统的控制律如下:

$$u_i(t) = \begin{cases} 0, & t \le T_e \\ \dfrac{1}{b_i}\alpha_{i,n}(t), & t > T_e \end{cases} \tag{29}$$

其中, $\alpha_{i,n}(t)$ 在式 (28) 中给出, T_e 为满足式 (7) 的常数.

4.2 稳定性分析

至此, 关于受攻击信息物理系统 (1), 其有限时间安全控制问题可解, 可总结为如下定理.

定理 2. 针对含有攻击的信息物理系统 (1)、分布式输出预选器 (4)、分布式有限时间观测器 (6) 以及分布式有限时间控制器 (29). 当条件 1 成立且 T_e 和 $\bar{\boldsymbol{M}}_i$ 分别满足式 (7) 和式 (8) 时, 信息物理系统 (1) 中状态 $x_{i,1}(t)$, 可以在有限时间内准确跟踪上任意信号 $x_{i,d}(t)$, 即存在 $T_c>0$, 当 $t \ge T_c+T_e$ 时,

$$x_{i,1}(t) = x_{i,d}(t) \tag{30}$$

其中, T_e 为满足 (7) 的常数, $T_c = \frac{2+\tau}{\tau\lambda}[V_n(0)]^{\frac{\tau}{2+\tau}}$, 而 $V_n(0)$ 为选择的 Lyapunov 函数初值; $\tau = \hbar_1/\hbar_2$ 而 $\hbar_1$ 为一偶数, $\hbar_2$ 为一奇数, 且 $0<\tau<\frac{1}{n+1}$; $\lambda = \frac{1}{2}(\gamma)^{\frac{2}{2+\tau}}$, $\gamma>0$ 为一常数.

证明. 首先证明, 含有攻击的信息物理系统 (1)、分布式输出预选器 (4)、分布式有限时间观测器 (6) 以及分布式有限时间控制器 (29) 是有限时间稳定的. 现在根据定理 2, 利用信息物理系统 (1), 分布式输出预选器 (4), 分布式有限时间观测器 (6), 当 $t \ge T_e$ 时, $\boldsymbol{x}_i(t) = \hat{\boldsymbol{x}}_i(t)$. 这就意味着, 当 $t \ge T_e$ 时, 可直接利用 $\hat{\boldsymbol{x}}_i(t)$ 代替 $\boldsymbol{x}_i(t)$, 进行控制器设计. 所以, 仅需分析 $t \ge T_e$ 时控制律的效果.

当 $t \ge T_e$ 时, 构造 Lyapunov 函数 $V_{i,n}(t) = V_{i,n-1}(t) + \int_{\alpha_{i,n-1}}^{e_{i,n}}[s^{\frac{1}{r_n}} - (\alpha_{i,n-1})^{\frac{1}{r_n}}]^{2-r_n+\tau}\mathrm{d}s$, 对其求导, 并考虑系统模型 (1) 和控制律 (29), 可得:

$$\dot{V}_{i,n}(t) = \dot{V}_{i,n-1}(t) + [(e_{i,n})^{\frac{1}{r_n}} - (\alpha_{i,n-1})^{\frac{1}{r_n}}]^{2-r_n+\tau}.$$
$$(b_iu_i + \sum_{j=1}^{n}\vartheta_{i,n,j}x_{i,j} + f_i - x_{i,d}^{(n)}) \le$$
$$-\beta_{i,n}\xi_{i,n}^2 + \xi_{i,n-1}^{2-r_n}(e_{i,n}-\alpha_{i,n-1}) -$$
$$2(\xi_{i,1}^2+\cdots+\xi_{i,n-1}^2) \tag{31}$$

根据杨氏不等式, 可得:

$$\xi_{i,n-1}^{2-r_n}(e_{i,n}-\alpha_{i,n-1}) \le 2^{1-r_{n-1}-\tau}|\xi_{i,n-1}|^{2-r_{n-1}-\tau}.$$
$$|\xi_{i,n}|^{r_n} \le \frac{1}{2}\xi_{i,n-1}^2 + c_{i,n}\xi_{i,n}^2 \tag{32}$$

选择 $\beta_{i,n} \ge c_{i,n}+1$, 并将式 (32) 代入式 (31), 可得:

$$\dot{V}_{i,n}(t) \le -2(\xi_{i,1}^2+\cdots+\xi_{i,n-1}^2) + \frac{1}{2}\xi_{i,n-1}^2 + c_{i,n}\xi_{i,n}^2 - \beta_{i,n}\xi_{i,n}^2 \le -(\xi_{i,1}^2+\cdots+\xi_{i,n}^2) \tag{33}$$

另外, 与式 (21) 相似, 可得:

$$|e_{i,j}-\alpha_{i,j-1}| \le 2^{2-r_j}|\xi_{i,j}|^{r_j} \tag{34}$$

进而, 可得:

$$\int_{\alpha_{i,j-1}}^{e_{i,j}}[s^{\frac{1}{r_j}} - (\alpha_{i,j-1})^{\frac{1}{r_j}}]^{2-r_j+\tau}\mathrm{d}s \le$$
$$|e_{i,j}-\alpha_{i,j-1}|\left|(e_{i,j})^{\frac{1}{r_j}} - (\alpha_{i,j-1})^{\frac{1}{r_j}}\right|^{2-r_j+\tau} \le$$
$$2^{2-r_j}|\xi_{i,j}|^{r_j}|\xi_{i,j}|^{2-r_j+\tau} = 2^{2-r_j}|\xi_{i,j}|^{2+\tau} \tag{35}$$

那么, 根据 $V_{i,n}(t)$ 定义, 可得:

$$V_{i,n}(t) \le \frac{1}{\gamma_i}(\xi_{i,1}^{2+\tau}+\cdots+\xi_{i,n}^{2+\tau}) \tag{36}$$

其中, $\gamma_i \ge 0$ 为一常数.

进而, 构造 Lyapunov 函数 $V_n(t) = \sum_{i=1}^{N}V_{i,n}(t)$, 对其求导, 可得:

$$\dot{V}_n(t) \le -\sum_{i=1}^{N}(\xi_{i,1}^2+\cdots+\xi_{i,n}^2) \tag{37}$$

注意, 当 $\lambda_i = \frac{1}{2}(\gamma_i)^{\frac{2}{2+\tau}}$ 时, $\lambda_i(V_{i,n})^{\frac{2}{2+\tau}} = \lambda_i\frac{1}{(\gamma_i)^{\frac{2}{2+\tau}}}(\xi_{i,1}^2+\cdots+\xi_{i,n}^2) \le \frac{1}{2}(\xi_{i,1}^2+\cdots+\xi_{i,n}^2)$. 那定义 $\gamma = \min\{\gamma_i\}$, 并选取 $\lambda = \frac{1}{2}(\gamma)^{\frac{2}{2+\tau}}$, 可得:

$$\dot{V}_n(t)+\lambda[V_n(t)]^{\frac{2}{2+\tau}}\le-\sum_{i=1}^{N}(\xi_{i,1}^2+\cdots+\xi_{i,n}^2)+\lambda\frac{1}{\gamma^{\frac{2}{2+\tau}}}\sum_{i=1}^{N}(\xi_{i,1}^2+\cdots+\xi_{i,n}^2)\le-\frac{1}{2}\sum_{i=1}^{N}(\xi_{i,1}^2+\cdots+\xi_{i,n}^2)\tag{38}$$

由于 $\xi_{i,j}^2\ge 0$, 则有 $\dot{V}_n(t)+\lambda[V_n(t)]^{\frac{2}{2+\tau}}\le 0$; 求解该方程可得 $V_n(t)\le-\frac{t\tau\lambda}{2+\tau}+[V_n(0)]^{\frac{\tau}{2+\tau}}$. 注意, 根据定义 $V_n(t)\ge 0$, 那当 $t\ge T_c$ 时, $V_n(t)\equiv 0$. 因此可得, 包含攻击的信息物理系统 (1)、分布式输出预选器 (4)、分布式有限时间观测器 (6) 以及分布式有限时间控制器 (29) 的整个闭环系统是有限时间稳定的, 即存在 $T_c>0$, 当 $t\ge T_c$ 时, $x_{i,1}(t)=x_{i,d}(t)$.

接下来, 将证明当 $t\in[0,T_c]$ 时, 系统中的各个变量不会发散. 构造函数 $\Theta_i(\boldsymbol{e}_i)=\frac{1}{2}(e_{i,1}^2+\cdots+e_{i,n}^2)$, 计算其导数可得:

$$\dot{\Theta}_i(\boldsymbol{e}_i,t)=e_{i,1}e_{i,2}+\cdots+e_{i,n}\cdot[b_iu_i+\sum_{j=1}^{n}\vartheta_{i,n,j}x_{i,j}+f_i-x_{i,d}^{(n)}]\tag{39}$$

令 $\varepsilon_i(t)=\sum\limits_{j=1}^{n}\vartheta_{i,n,j}x_{i,j}(t)+f_i(\bar{x},t)+b_iu_i(t)-x_{i,d}^{(n)}(t)$, 根据控制律定义式 (29) 以及式 (28), 可得:

$$\varepsilon_i(t)\le\beta_{i,n}|e_{i,n}|^{\frac{r_{n+1}}{r_n}}+\beta_{i,n}|\alpha_{i,n-1}|^{\frac{r_{n+1}}{r_n}}\le\beta_{i,n}\cdot|e_{i,n}|^{\frac{r_{n+1}}{r_n}}+\beta_{i,n}\beta_{i,n-1}^{\frac{r_{n+1}}{r_n}}|e_{i,n-1}|^{\frac{r_{n+1}}{r_{n-1}}}+\cdots+\beta_{i,n}\beta_{i,n-1}^{\frac{r_{n+1}}{r_n}}\cdots\beta_{i,1}^{\frac{r_{n+1}}{r_2}}|e_{i,1}|^{\frac{r_{n+1}}{r_1}}\tag{40}$$

下面的讨论分为 $e_{i,1}^2+\cdots+e_{i,n}^2\ge 1$ 和 $e_{i,1}^2+\cdots+e_{i,n}^2<1$ 两种情况. 首先, 当 $e_{i,1}^2+\cdots+e_{i,n}^2\ge 1$ 时, 由于 $\frac{r_{n+1}}{r_j}=\frac{1-n\tau}{1-(j-1)\tau}<1$, 根据式 (40), 即有

$$\varepsilon_i(t)\le\upsilon_i(|e_{i,n}|+\cdots+|e_{i,1}|)\tag{41}$$

其中, $\upsilon_i=\beta_{i,n}+\cdots+\beta_{i,n}\beta_{i,n-1}^{\frac{r_{n+1}}{r_n}}\cdots\beta_{i,1}^{\frac{r_{n+1}}{r_2}}$.

将式 (41) 代入式 (39), 可得:

$$\dot{\Theta}_i(\boldsymbol{e}_i,t)+\upsilon_i|e_{i,n}|(|e_{i,n}|+\cdots+|e_{i,1}|)\le\frac{1}{2}(e_{i,1}^2+e_{i,2}^2)+\cdots+\frac{1}{2}(e_{i,n-1}^2+e_{i,n}^2)+\frac{\upsilon_i}{2}(e_{i,1}^2+e_{i,n}^2)+\cdots+\upsilon_ie_{i,n}^2\le(1+n\upsilon_i)(e_{i,1}^2+\cdots+e_{i,n}^2)=K_i\Theta_i(e_i,t)\tag{42}$$

其中, $K_i=2(1+n\upsilon_i)$.

另外, 当 $e_{i,1}^2+\cdots+e_{i,n}^2\le 1$ 时, 则 $|x_{i,j}|<1$, 根据式 (40), 即有:

$$\alpha_{i,n}(t)\le\upsilon_i(|e_{i,n}|+\cdots+|e_{i,1}|)\le\upsilon_i\tag{43}$$

此时, 将式 (43) 代入式 (39), 可得:

$$\dot{\Theta}_i(\boldsymbol{e}_i,t)\le|e_{i,1}||e_{i,2}|+\cdots+|e_{i,n-1}||e_{i,n}|+\upsilon_i|e_{i,n}|\le L_i\tag{44}$$

其中, $L_i=n-1+\upsilon_i$.

综合式 (42) 和式 (44), 可得:

$$\dot{\Theta}_i(\boldsymbol{e}_i,t)\le K_i\Theta_i(\boldsymbol{e}_i,t)+L_i\tag{45}$$

那么, 构造函数 $\Theta(\boldsymbol{e})=\sum_{i=1}^{N}\Theta_i(\boldsymbol{e}_i)$, 并根据式 (45), 可求得 $\Theta(\boldsymbol{e})$ 的导数为

$$\dot{\Theta}(\boldsymbol{e})\le K\Theta(\boldsymbol{e},t)+L\tag{46}$$

其中, $K=\max\{K_i\}$ 和 $L=\max\{L_i\}$. 求解不等式 (46), 可得:

$$\Theta(\boldsymbol{e},t)\le\left[\Theta(\boldsymbol{e}(0)+\frac{L}{K}\right]\mathrm{e}^{Kt}-\frac{L}{K}\tag{47}$$

根据 $\Theta(\boldsymbol{e})$ 的定义, 可得, 在 $t\in[0,T_c]$ 时, 系统 (1) 中各子系统的状态 $x_i(t)$ 都是有界的. □

5 仿真示例

为了验证本文提出算法的有效性, 将其应用到如图 2 所示的微电网系统中的二次频率恢复控制中[18]. 该微电网包含 4 个发电机, 4 个局部负载以及 3 组传输母线. 遵照该文方法, 仅考虑发电过程, 而将原电机的机械力矩直接作为发电机受控输入, 且当传输母线为无损时, 则第 i 个发电机的相位下降过程为

$$\begin{cases}\dot{\delta}_i(t)=\omega_i(t)\\ \tau_{Pi}\dot{\omega}_i(t)+\omega_i(t)+k_{Pi}(P_i(t)-P_i^d(t))+u_i(t)=0\end{cases}\tag{48}$$

其中, $\delta_i(t)$ 是第 i 个发电机的电气角, $\omega_i(t)$ 是相对角速度, $u_i(t)$ 是设计的受控输入, τ_{Pi} 为测量有功功率的滤波器系数, k_{Pi} 为频率下降增益; $P_i^d(t)$ 为期望的有功功率, $P_i(t)$ 而为实际的有功功率, 它满足如下条件:

$$P_i(t)=P_{1i}V_i^2(t)+P_{2i}V_i(t)+P_{3i}+\sum_{j=1}^{N}V_i(t)V_j(t)|B_{ij}|\sin(\delta_i-\delta_j)\tag{49}$$

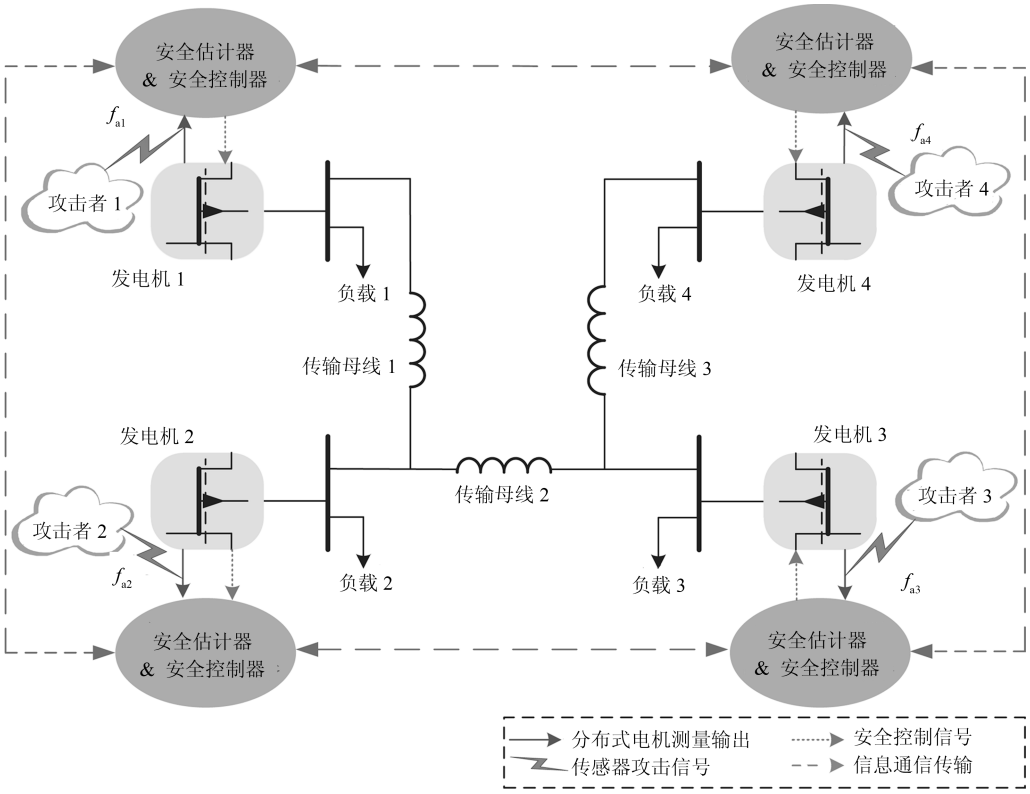


图 2　受到传感器攻击的微电网系统框图

Fig. 2　The diagram of the micro-grid system under sensor attacks

其中, B_{ij} 是通过剔除所有物理母线后得到的内部网络节点后得到的阻抗矩阵的第 i 行第 j 列的参数; $V_i(t)$ 为第 i 个发电机的电压, P_{1i}、P_{2i} 和 P_{3i} 分别为名义恒定阻抗、恒定电流和恒定功率负载. 该微电网的参数见表 1.

表 1　微电网系统模型参数

Table 1　Parameters of isolated grids systems

		发电机 1	发电机 2	发电机 3	发电机 4
模型	τ_{Pi}	0.016	0.016	0.016	0.016
	k_{Pi}	6E−5	3E−5	2E−5	1.5E−5
负载	P_{1i}	0.01	0.01	0.01	0.01
	P_{2i}	1	2	3	4
	P_{3i}	1E−4	1E−4	1E−4	1E−4
母线	$B_{12}=10\,\Omega^{-1}$, $B_{23}=10.67\,\Omega^{-1}$, $B_{34}=9.82\,\Omega^{-1}$				
参考电气角	δ_i^d=1 (rad)				

选取 $\boldsymbol{x}_i(t)=[\delta_i(t),\omega_i(t)]^{\mathrm{T}}$ 作为系统状态, 将式 (49) 代入式 (48), 可得形如式 (1) 的模型.

$$\begin{cases}\dot{\boldsymbol{x}}_i(t)=A_i\boldsymbol{x}_i(t)+B_iu_i(t)+B_if_i(\bar{\boldsymbol{x}},t)\\ \boldsymbol{y}_i(t)=C_i\boldsymbol{x}_i(t)+\boldsymbol{\eta}_i(t)\end{cases}\tag{50}$$

其中, A_i 和 B_i 的值可以通过表 1 计算可得, 选择 $C_i=[1\,0;1\,0;1\,0]$; $f_i(\bar{\boldsymbol{x}}_i,t)=f_{i0}/\tau_{Pi}$ 而 $f_{i0}=P_{1i}V_i^2(t)+P_{2i}V_i(t)+P_{3i}-P_i^d+\sum\limits_{j=1}^{N}V_i(t)V_j(t)\,|B_{ij}|\sin(x_{i,1}-x_{j,1})$, $\boldsymbol{\eta}_i(t)$ 为注入的传感器攻击. 设计的攻击信号为: $\eta_{1,3}(t)=[1\,0]\,\mathrm{e}^{A_1t}$, $\eta_{2,1}(t)=[1\,0]\,\mathrm{e}^{A_2t}$, $\eta_{3,2}(t)=[10]\,\mathrm{e}^{A_3t}$ 和 $\eta_{4,1}(t)=[1\,0]\,\mathrm{e}^{A_4t}$, 其余分量为 0.

根据第 3 节和第 4 节的分析, 设计的有限时间观测器参数为 $T_e=0.45$, $\bar{F}_i=[-17.5\quad 1.0\quad 0\quad 0;-2\,106.3\quad -62.5\quad 0\quad 0;\ 0\quad 0\quad 42.5\quad 1.0;\ 0\quad 0\quad -2\,856.3\quad -62.5]$, $\bar{L}_i=[17.5\;2\,106.3\;-42.5\;2\,856.3]^{\mathrm{T}}$, $\bar{M}_i=[1.0\;0\;0\;0;0\;1.0\;0\;0]$; 而安全控制器的参数为 $h_{i,1}=2$ 和 $h_{i,2}=7$, $\beta_{i,1}=5$ 和 $\beta_{i,2}=2.5$.

仿真结果见图 3 ∼ 图 7. 发电机组的状态及其估计如图 3 ∼ 图 6 所示, 可以看出, 经过 $T_e=0.45\,\mathrm{s}$ 后, 所有发电机的状态估计值与真实值完全一致, 这就验证了文中理论分析的有效性; 此外, 利用设计的安全控制器, 每个发电机的电气角都在有限时间, 大约为 2.7 s 后, 达到期望的角度, 见图 3 ∼ 图 6; 同样, 从图 3 ∼ 图 6 可以看出, 每个发电机的状态都是有界的, 同时根据图 7 可得, 设计的安全控制信号也是有界的, 这同样也验证了本文的理论分析.

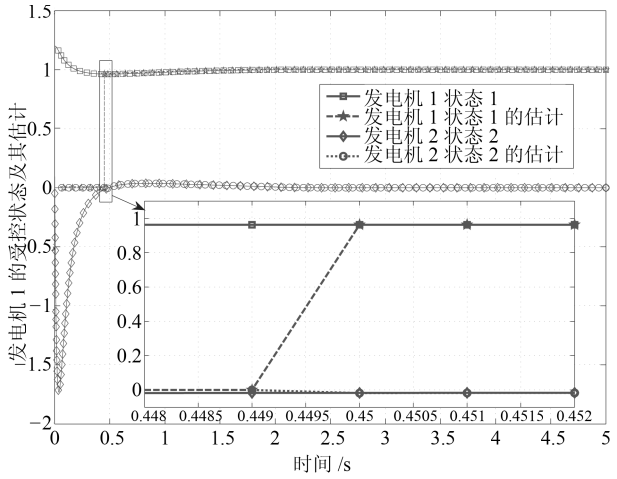


图 3 发电机 1 受控状态及其估计值

Fig. 3 The angle of the 1st generator and its estimation

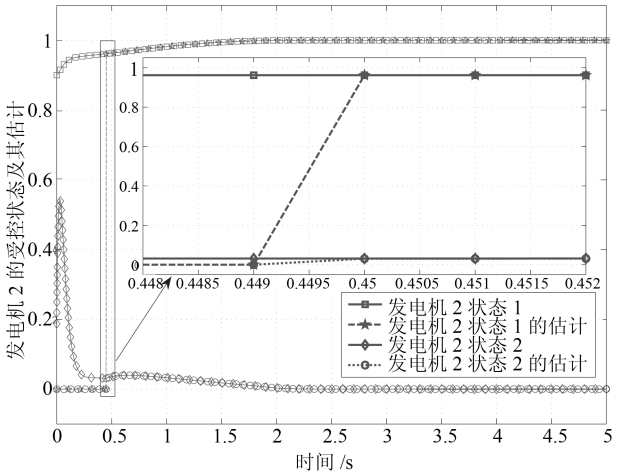


图 4 发电机 2 受控状态及其估计值

Fig. 4 The angle of the 2nd generator and its estimation

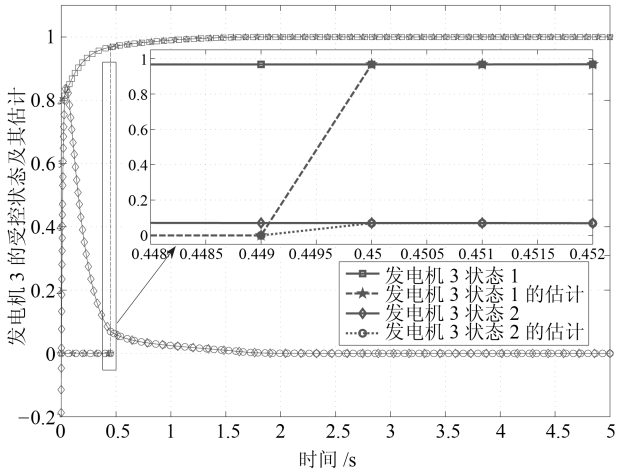


图 5 发电机 3 受控状态及其估计值

Fig. 5 The angle of the 3rd generator and its estimation

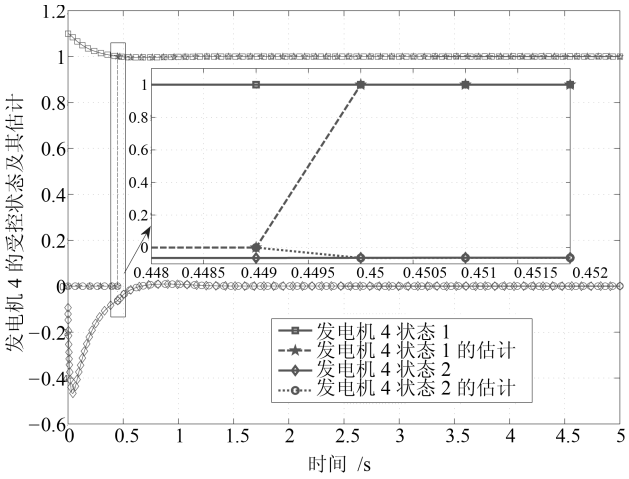


图 6 发电机 4 受控状态及其估计值

Fig. 6 The angle of the 4th generator and its estimation

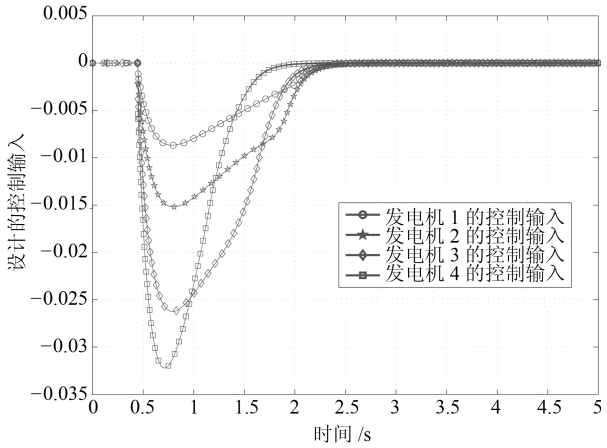


图 7 设计的安全控制输入

Fig. 7 The designed secure control law

6 结束语

本文针对含有非线性耦合特性的受攻击信息物理系统, 研究其有限时间状态安全估计以及分布式有限时间安全控制器设计问题. 首先, 设计一种由安全测量预选器和有限时间观测器组成的分布式安全状态估计策略, 能够保证在预设时间内实现有限时间安全状态估计; 其次, 利用获得的安全状态估计, 并采用反步设计方法, 提出一种分布式有限时间安全控制器, 可以保证系统的在有限时间内跟踪期望信号; 并将文中提出的方法在一个微电网系统中进行仿真实验, 其结果验证了所提方法的有效性. 需要说明的是, 本文涉及发电过程没有涉及对机械传动过程, 即对原动机的工作特性研究有所不足, 因此, 在将本文提出的方法应用到实际系统时, 还有不少工作需要完成. 此外, 实际系统中还需要关注系统不确定性、噪声、状态及控制信号约束等特性, 这也是我们未来研究的目标.

References

1 Park K J, Zheng R, and Liu X. Cyber-physical systems: Milestones and research challenges. *Computer Communications*, 2012, **36**(1): 1−7

2 Conti J P. The day the samba stopped. *Engineering & Technology*, 2010, **25**(4): 46−47

3 Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 2011, **9**(3): 49−51

4 Pasqualetti F, Dörfler F, and Bullo F. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 2013, **58**(11): 2715−2729

5 Ao W, Song Y and Wen C. Adaptive cyber-physical system attack detection and reconstruction with application to power systems. *IET Control Theory & Applications*, 2016, **10**(12): 1458−1468

6 Chen Y, Kar S, and Moura J M. Dynamic attack detection in cyber-physical systems with side initial state information. *IEEE Transactions on Automatic Control*, 2017, **62**(9): 4618−4624

7 Fawzi H, Tabuada P, and Diggavi S. Secure state-estimation for dynamical systems under active adversaries. In: Proceeding of Forty-Ninth Annual Allerton Conference. Monticello, USA: IEEE, 2011. 337−344

8 Fawzi H, Tabuada P, and Diggavi S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, 2014, **59**(6): 1454−1467

9 Shoukry Y and Tabuada P. Event-triggered state observers for sparse sensor noise/attacks. *IEEE Transactions on Automatic Control*, 2016, **61**(8): 2079−2091

10 Shoukry Y, Chong M, Wakaiki M, Nuzzo P, Sangiovanni-Vincentelli A L, Seshia S A, Hespanha J P and Tabuada P. Smt-based observer design for cyber-physical systems under sensor attacks, In: Proceeding of 7th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). IEEE Computer Society, 2016. 1−10

11 Ao W, Song Y, Wen C, and Lai J. Finite time attack detection and supervised secure state estimation for CPSs with malicious adversaries. *Information Sciences*, 2018, **451-452**: 67−82

12 Ao W, Song Y and Wen C. Distributed secure state estimation and control for CPSs under sensor attacks. *IEEE Transactions on Cybernatics*, 2018, DOI: 10.1109/TCYB.2018.2868781

13 Wang Y, Song Y, Gao H and Lewis F L. Distributed fault-tolerant control of virtually and physically interconnected systems with application to high-speed trains under traction/braking failures. *IEEE Transactions on Intelligent Transportation Systems*, 2016, **17**(2): 535−545

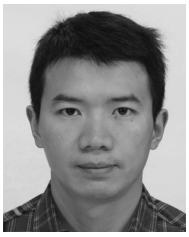
14 Mo Y, Hespanha J P, and Sinopoli B. Resilient detection in the presence of integrity attacks. *IEEE Transactions on Signal Processing*, 2014, **62**(1): 31−43

15 Mo Y and Sinopoli B. Secure estimation in the presence of integrity attacks. *IEEE Transactions on Automatic Control*, 2015, **60**(4): 1145−1151

16 Engel R and Kreisselmeier G. A continuous-time observer which converges in finite time. *IEEE Transactions on Automatic Control*, 2002, **47**(7): 1202−1204

17 Li S, Sun H, Yang J, and Yu X. Continuous finite-time output regulation for disturbed systems under mismatching condition. *IEEE Transactions on Automatic Control*, 2015, **60**(1): 277−282

18 Guo F, Wen C, Mao J and Song Y. Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids. *IEEE Transactions on Industrial Electronics*, 2015, **62**(7): 4355−4364



敖 伟 重庆科技学院数理与大数据学院副教授. 2003 年获得国防科技大学自动化学士学位, 2017 年获得重庆大学控制理论与控制工程博士学位. 主要研究方向为自适应控制, 容错控制, 信息物理系统攻击监测与安全控制.
E-mail: craneaow@cqu.edu.cn

(**AO Wei** Associate professor at the School of mathematics, Physics and Big-data of the Chongqing Unversity of Science and Technology. He received his bachelor degree from the National University of Defense Technology in 2003 and Ph. D. degree in Control Theory and Control Engineering from Chongqing University in 2017. His research interest covers adaptive control, fault tolerant control, attack detection, and secure control of cyber-physical systems.)

宋永端 中国自动化学会常务理事, 中国自动化学会 "可信控制系统" 专委会主任, IEEE CIS 重庆计算智能分会主席, 任包括 *IEEE Translation on Automatic Control* 在内的 6 部国际学术杂志编委. 1992 年获得田纳西理工大学电气与计算机博士学位. 主要研究方向为智慧系统, 导航与控制, 仿生自适应控制, 系统安全与控制. 本文通信作者. E-mail: ydsong@cqu.edu.cn

(**SONG Yong-Duan** He is the standing director of Automation Association of China and the chair of the committee on Reliable Control Systems under Automation Association of China. He is also the founding chair of the Chongqing Chapter of IEEE Computational Intelligence Society (CIS). He is serving as an Associate Editor for 6 international scientific journals including *IEEE Translation on Automatic Control*. He received his Ph. D. degree in electrical and computer engineering from Tennessee Technological University, Cookeville, TN, USA in 1992. His research interest covers intelligent systems, guidance navigation and control, bioinspired adaptive control, system cooperation and reliability. Corresponding author of this paper.)

温长云 新加坡南洋大学终身教授. 1983 年 7 月获得西安交通大学学士学位, 1990 年 2 月获得澳大利亚纽卡斯尔大学博士学位, 1989 年 8 月至 1991 年 8 月在澳大利亚阿德莱德大学从事博士后研究, 1991 年 8 月加入新加坡南洋理工大学. IEEE 会士, 2011 年～2013 年担任 IEEE 会士委员会委员, 2010 年～2013 年 IEEE 控制系统协会卓越讲座人; 曾获 2005 年新加坡工程师学会卓越工程成就奖, 2017 年 *IEEE Transactions on Industrial Electronics* 最佳论文奖等. 曾任/担任包括*IEEE Trans. Automatic Control* (2000～2002), Automatica (从 2006 年起), *IEEE Trans. Industrial Electronics* (从 2013 年起), *IEEE Control Systems Magazine* (从 2009 年起) 等国际学术期刊编委. 主要研究方向为自适应控制, 自主机器人系统, 智慧电能管理系统复杂网络系统控制, 信息物理系统. E-mail: ecywen@ntu.edu.sg

(**WEN Chang-Yun** Full prafessor at Nanyang Technological University, Singapore. He received his bachelor degree from Xi′an Jiaotong University, Xi′an, China, in July 1983, and the Ph. D. degree from the University of Newcastle, Australia, in February 1990. From August 1989 to August 1991, he was a Postdoctoral Fellow at the University of Adelaide, Australia. He joined the Nanyang Technological University, Singapore in August 1991, where he has been a tenured Full Professor since 2008. He was/has been an Associate Editor of a number of journals including IEEE Trans. Automatic Control (2000～2002), Automatica (since 2006), IEEE Trans. Industrial Electronicsv (since 2013), IEEE Control Systems Magazine (since 2009) etc. He is a Fellow of IEEE, was a Member of the IEEE Fellow Committee from January 2011 to December 2013 and a Distinguished Lecturer of IEEE Control Systems Society from 2010 to 2013. He was awarded the IES Prestigious Engineering Achievement Award 2005 by the Institution of Engineers, Singapore (IES) in 2005. He received the Best Paper Award of IEEE Transactions on Industrial Electronics in 2017. His research interest covers adaptive control, autonomous robotic system, intelligent power management system, complex systems and networks.)