恶意攻击下基于分布式稀疏优化的安全状态估计

张岱峰 [1] 段海滨 [1, 2]

摘 要 恶意生成的量测攻击信号是导致信息物理系统 (Cyber-physical system, CPS) 探测失效的主要原因, 如何有效削弱其影响是实现精准探测、跟踪与感知的关键问题. 分布式传感器网络 (Distributed sensor network, DSN) 依靠多传感器协作与并行处理突破单一监测节点的任务包线, 能够显著提升探测系统跟踪精度与可靠性. 首先, 依据压缩感知理论, 将单一节点的目标运动状态估计建模为一种基于 l_0 范数最小化的稀疏优化问题, 采用正交匹配追踪法 (Orthogonal matching pursuit, OMP) 重构量测攻击信号, 以克服采用凸优化算法求解易陷入局部最优的缺陷. 通过卡尔曼滤波量测更新抵消攻击信号影响, 恢复目标运动的真实状态. 其次, 针对错误注入攻击等复杂量测攻击形式, 基于势博弈理论, 提出一种分布式稀疏优化安全状态估计方法, 利用多传感器节点信息交互与协作提升探测与跟踪的稳定性. 仿真结果表明, 所提方法在分布式传感器网络协作抵抗恶意攻击方面具有优越性.

关键词 恶意攻击, 分布式安全状态估计, 稀疏优化, 势博弈

引用格式 张岱峰, 段海滨. 恶意攻击下基于分布式稀疏优化的安全状态估计. 自动化学报, 2021, **47**(4): 813−824

DOI 10.16383/j.aas.c200276

Secure State Estimation Based on Distributed Sparse Optimization Under Malicious Attacks

ZHANG Dai-Feng[1] DUAN Hai-Bin[1, 2]

Abstract Malicious attacks against the measurements is one of the primary cause accounting for the detection failure of cyber-physical systems (CPS). Reducing the impact of measurement attack is a key problem of the accurate detection, target tracking, and sensing for CPS. Distributed sensor networks (DSN) are able to break through the task envelope of single surveillance node through coordination and parallel processing and thus remarkably improve the tracking performance and reliability of detection systems. Based on the compressive sensing theory, the state estimation for single-plant target tracking is modelled as an l_0-norm minimization problem, which is also equivalent to a sparse optimization problem. Under sparse malicious attacks, the orthogonal matching pursuit (OMP) is utilized to reconstruct the attack signals and to avoid the local optima induced by the convex optimization algorithms. A combined Kalman filter is presented to obtain the true target information where the attack signals are compensated in the measurement update. Then, a distributed secure state estimation method based on the potential game theory is proposed in view of the complex attacks such as the false data injection, where a potential game framework is established to enhance the stability of target tracking by the information exchange and coordination among neighboring sensors. Simulation results demonstrate the effectiveness of the proposed method against the sparse malicious attacks on DSNs.

Key words Malicious attack, distributed secure state estimation, sparse optimization, potential game

Citation Zhang Dai-Feng, Duan Hai-Bin. Secure state estimation based on distributed sparse optimization under malicious attacks. *Acta Automatica Sinica*, 2021, **47**(4): 813−824

收稿日期 2020-05-02 录用日期 2020-08-14
Manuscript received May 2, 2020; accepted August 14, 2020
国家自然科学基金 (U20B2071, 91948204, U1913602, U19B2033), 科技创新 2030 "新一代人工智能"重大项目 (2018AAA0102303), 航空科学基金 (20185851022) 资助
Supported by National Natural Science Foundation of China (U20B2071, 91948204, U1913602, U19B2033), Science and Technology Innovation 2030-Key Project of "New Generation Artificial Intelligence" (2018AAA0102303), and Aeronautical Science Foundation of China (20185851022)
本文责任编委 孙秋野
Recommended by Associate Editor SUN Qiu-Ye
1. 北京航空航天大学自动化科学与电气工程学院仿生自主飞行系统研究组 北京 100083 2. 鹏城实验室 深圳 518000
1. Bio-inspired Autonomous Flight Systems Research Group, School of Automation Science and Electrical Engineering, Beihang University, Beijing 100083 2. Peng Cheng Laboratory, Shenzhen 518000

信息物理系统[1−2] (Cyber-physical system, CPS) 正在成为推动新一代工业技术发展, 加速 "工业 4.0"时代进程的核心力量[3]. 作为一类典型的 CPS, 无线传感器网络 (Wireless sensor network, WSN) 在军事、工业和消费等领域具有广泛的应用, 如目标监测、区域监控等[4−5]. 然而, 受制于通信带宽及传输方式, 在实际应用中, WSN 容易遭受恶意攻击[6−8], 例如量测信号受到噪声或错误数据注入攻击 (False data injection, FDI)[7−8], 会严重降低其监测效能. 此外, 在军事领域特别是电磁作战过程中, 雷达易受到敌方干扰机的影响, 导致回波信号偏离真实目标移动轨迹, 从而降低雷达探测能力[9]. 在恶意

攻击条件下, 单一传感器节点已难以克服量测攻击的破坏性影响, 尤其在 FDI 攻击条件下, 传感器不易识别该类注入信号从而造成监测数据严重偏离真实目标状态. 分布式传感器网络 (Distributed sensor network, DSN) 相比单一节点的优势在于, 其能够利用多节点并行观测及节点间信息融合生成更为可靠的目标跟踪与环境监测数据. 由于恶意攻击难以作用于多个节点, 这就使 DSN 利用局部通信和高置信节点构建安全状态估计成为可能[10]. 因此, 研究恶意攻击下的分布式安全状态估计问题, 对于提升 CPS 与 WSN 的探测与跟踪稳定性, 增强其复杂环境作业功效具有重要的现实意义.

近年来, 关于 CPS 的安全估计问题受到国内外学者广泛关注. Manandhar 等[11] 通过在卡尔曼滤波框架中融入卡方检测器对 CPS 中的虚假攻击信息进行检测, 进而排除系统故障. Li 等[12] 从博弈论角度将安全估计问题建模为一种零和博弈过程, 通过求取纳什均衡获得在有限能量条件下的最优状态估计策略. Kwon 等[13] 提出了一种组合鲁棒控制器, 在考虑多种量测攻击形式的基础上, 通过调节子控制系统实现对不同种类攻击信号的抑制. 周雪等[14] 设计了一种基于事件触发机制的分布式扩展卡尔曼滤波器, 在恶意攻击信号存在有限上界的情况下, 保证系统能够达到一定的安全估计精度. 上述工作均在一定程度上对量测攻击信号作出了先验性假设 (如时不变性, 分布特征, 攻击信号边界等). 然而, 在实际过程中, 恶意攻击信号的形式可能是未知的、不确定的, 这就需要考虑更为实际的安全估计问题.

Fawzi 等[15] 从理论上分析了一个线性时不变系统能够承受的最大攻击次数, 而不考虑具体攻击形式. 在此基础上, 将安全估计问题等效为 l_1 范数凸优化问题, 采用压缩感知原理重构量测攻击条件下的真实状态. Chang 等[16] 在上述工作基础上进一步考虑时变攻击策略, 提出了一种适应于更一般约束环境的 l_1 范数凸优化估计方法. Shoukry 等[17] 则将安全估计问题分别转为一种静态批处理优化问题 (Static batch optimization, SBO) 和一种类 Luenberger 观测器设计问题, 并针对性地提出两种基于事件驱动的安全估计模型用于求解上述问题. Wu 等[18] 则进一步考虑观测模型的输入不确定性, 提出一种滑模观测器用于解决同时存在量测攻击与输入不确定性的目标跟踪问题. 以上所述研究工作主要针对单一传感器节点的状态估计或目标跟踪效果, 未考虑 DSN 节点之间的协同作用. 然而, 鉴于 CPS 与 WSN 本身具备的分布式作业特点, 利用多传感器节点之间的信息交互, 从中筛选信息可靠的传感器节点并进行针对性数据融合, 能够在很大程度上提升 DSN 的状态估计稳定性. 典型实例如文献 [8] 中采用了一种安全扩散极小均方差算法 (Secure diffusion least-mean squares, S-dLMS), 通过筛选和融合具备可靠置信度的邻居信息提升 DSN 系统的状态跟踪稳定性. 此外, Liang 等[19] 也提出了一种基于置信度判别的分布式卡尔曼滤波方法用以实现稀疏攻击条件下的目标跟踪, 该方法通过聚类方式筛选未受攻击的传感器节点, 并通过数据共享提升 DSN 的整体效能.

本文考虑恶意攻击条件下的离散线性空间 DSN 安全状态估计问题, 提出一种分布式稀疏优化估计方法. 主要贡献包括:

1) 借鉴压缩感知原理, 将线性空间目标跟踪安全估计问题建模为一种基于 l_0 范数的稀疏优化问题, 采用正交匹配追踪法 (Orthogonal matching pursuit, OMP) 重构攻击信号, 结合卡尔曼滤波求解观测目标的真实运动状态. 现有多数工作将上述问题转为凸优化模型求解[15−18], 为降低计算复杂度, 凸优化算法常采用启发式结构, 致使结果容易陷入局部最优, 在较短时限内不易收敛到精确解. 因此, 本文考虑到上述弊端, 将安全估计问题建模为稀疏优化问题, 利用解的稀疏性逼近真实攻击信号, 以提高求解质量.

2) 针对 DSN 架构, 考虑复杂攻击形式, 提出一种分布式稀疏优化安全估计方法, 利用相邻传感器之间信息交互与融合策略实施主动调节, 克服单一传感器节点安全估计不稳定的弊端, 提升网络整体融合效能. 基于势博弈理论设计了相邻传感器节点之间的融合决策, 对攻击信号预测值进行结构对比, 筛选高可靠节点. 该方法有效利用了稀疏攻击信号特征, 提供了一种更为简洁的可靠节点选择与数据融合机制, 与当下流行算法的对比仿真结果表明了所提方法的优越性.

符号说明: 如果 S 是一个集合, 则 $|S|$ 表示 S 的基数; 对于向量 $\boldsymbol{x}\in\mathbf{R}^n$, $\mathrm{supp}(\boldsymbol{x})$ 表示其支集, 即 $\mathrm{supp}(\boldsymbol{x})=\{i\leq n\,|x_i\neq 0\}$; 其 l_0 范数定义为 $\|\boldsymbol{x}\|_{l_0}:=|\mathrm{supp}\,(\boldsymbol{x})|$; 对于任意矩阵 $\boldsymbol{M}\in\mathbf{R}^{m\times n}$, $\mathrm{rowsupp}\,(\boldsymbol{M})=\{i\leq m|\boldsymbol{M}_i\neq 0\}$ 表示其非零行索引集合, 其中 $\boldsymbol{M}_i$ 为第 i 行向量; 矩阵 l_0 范数定义为 $\|\boldsymbol{M}\|_{l_0}:=|\mathrm{rowsupp}\,(\boldsymbol{M})|$; 若 $|\mathrm{supp}\,(\boldsymbol{x})|\leq k$, 则称 $\boldsymbol{x}$ 为 k-稀疏; 定义 $\mathcal{R}\,(\boldsymbol{M})$ 为矩阵 $\boldsymbol{M}$ 的值域空间, $\mathcal{N}\,(\boldsymbol{M})$ 为其零空间.

1 问题描述

本文针对离散线性空间下的 DSN 目标跟踪安全估计问题, 考虑以下目标运动模型

$$\boldsymbol{x}_{k+1}=\boldsymbol{A}\boldsymbol{x}_k+\boldsymbol{B}\boldsymbol{u}_k+\boldsymbol{w}_k \tag{1}$$

其中, $\boldsymbol{x}_k\in\mathbf{R}^n$ 与 $\boldsymbol{u}_k\in\mathbf{R}^m$ 分别为 k 时刻目标状态与控制量; $\boldsymbol{A}\in\mathbf{R}^{n\times n}$, $\boldsymbol{B}\in\mathbf{R}^{n\times m}$ 分别为状态转移矩阵和输入矩阵; $\boldsymbol{w}_k\in\mathbf{R}^n$ 表示 k 时刻运动过程零均值高斯白噪声, 其满足协方差矩阵 $\boldsymbol{Q}\in\mathbf{R}^{n\times n}$.

DSN 由 N 个传感器节点组成, 每个节点具有以下目标状态测量方程

$$\boldsymbol{y}_k^{(i)}=\boldsymbol{C}^{(i)}\boldsymbol{x}_k^{(i)}+\boldsymbol{e}_k^{(i)}+\boldsymbol{v}_k^{(i)},\ \ i\in\{1,\,2,\cdots,\,N\} \tag{2}$$

其中, i 为节点编号; $\boldsymbol{y}_k^{(i)}\in\mathbf{R}^p$, $\boldsymbol{C}^{(i)}\in\mathbf{R}^{p\times n}$ 分别为 k 时刻节点 i 的量测输出与量测矩阵; $\boldsymbol{v}_k^{(i)}\in\mathbf{R}^p$ 表示 k 时刻节点 i 的量测零均值高斯白噪声, 协方差矩阵为 $\boldsymbol{R}^{(i)}\in\mathbf{R}^{m\times m}$; $\boldsymbol{e}_k^{(i)}\in\mathbf{R}^p$ 代表 k 时刻时变攻击信号. 为保证 DSN 系统对目标可观测, 本文假设目标采用状态反馈控制 $\boldsymbol{u}_k=\boldsymbol{G}\boldsymbol{x}_k$, 使 $(\boldsymbol{A}+\boldsymbol{B}\boldsymbol{G},\,\boldsymbol{C}_i)$ 构成稳定可观测对. 若无法实现上述配置, 则式 (2) 退变为节点 i 的可观测子空间模型. 同时, 假设 DSN 通信拓扑为连通图, 为简化表述, 本节后续忽略节点索引上标.

注 1. 对于非线性目标, 可通过计算非线性成分关于上一时刻状态估计值的一阶泰勒展开式获取雅可比矩阵取代式 (1)、式 (2) 中的 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$ 矩阵, 转为线性系统后应用所提方法进行安全状态估计.

定义 1[15]. 状态估计器 $\mathcal{D}\colon(\mathbf{R}^p)^T\to\mathbf{R}^n$ 能够在有限时间 T 内抵挡 q 个量测通道攻击, 当且仅当对任意初始状态 $\boldsymbol{x}_0\in\mathbf{R}^n$, 任意受攻击的量测通道集合 $K\subset\{1,\cdots,\,p\}$ 且 $|K|\le q$, 任意攻击序列 $\boldsymbol{e}_0,\cdots,\,\boldsymbol{e}_{T-1}$ 且 $\mathrm{supp}\,(\boldsymbol{e}_k)\subset K$, 均有 $\mathcal{D}(\boldsymbol{y}_0,\cdots,\,\boldsymbol{y}_{T-1})=\boldsymbol{x}_0$, $k\in\{0,\cdots,\,T-1\}$.

注 2. 不失一般性, 认为闭环状态过程配置的系统极点均为正实数, 即 $\bar{\boldsymbol{A}}=\boldsymbol{A}+\boldsymbol{B}\boldsymbol{G}$ 可逆, 则通过状态估计器 $\mathcal{D}$ 重构初始状态 $\boldsymbol{x}_0$ 与重构当前状态 $\boldsymbol{x}_{T-1}$ 在理论上是等效的.

命题 1[15]. 若存在状态估计器 $\mathcal{D}$ 能够在有限时间 T 内抵挡 q 个量测通道攻击, 则 $\mathcal{D}_0$ 是一种最优估计, 满足

$$\begin{aligned}\mathcal{D}_0:\ &\min_{\hat{\boldsymbol{x}}\in\mathbf{R}^n,\ \hat{K}\subset\{1,\cdots,\,p\}}\left|\hat{K}\right|\\&\mathrm{supp}\left(\boldsymbol{y}_k-\boldsymbol{C}\boldsymbol{A}^k\hat{\boldsymbol{x}}\right)\subset\hat{K}\\&k\in\{0,\cdots,\,T-1\}\end{aligned} \tag{3}$$

然而, 由于 $\mathcal{D}_0$ 涉及对集合操作不易求解, 若采用枚举法则会显著增加计算复杂度. 由定义 1 可知, 对于每个传感器节点, 状态估计器 $\mathcal{D}$ 需要从受攻击的量测信号集 $\{\boldsymbol{y}_k\}$ 中重构初始状态. 对于攻击者一方, 受其发射功率与作用距离的限制, 一般无法对所有节点实施同步攻击, 在攻击过程中也不会轻易改变攻击通道, 即一般情况下对量测通道的攻击为稀疏性攻击[20]. 定义误差堆叠向量 $\boldsymbol{E}_{q,\,T}=[\boldsymbol{e}_0;\cdots;\,\boldsymbol{e}_{T-1}]\in\mathbf{R}^{pT}$, 其中攻击信号 $\boldsymbol{e}_k$ 满足 $|\mathrm{supp}\,(\boldsymbol{e}_k)|\le q\le p$, 即为 q-稀疏误差向量. 若忽略量测噪声 $\boldsymbol{v}_k$, 通过堆叠历史量测数据得到

$$\begin{aligned}\boldsymbol{Y}:=&\begin{bmatrix}\boldsymbol{y}_0\\\boldsymbol{y}_1\\\vdots\\\boldsymbol{y}_{T-1}\end{bmatrix}=\begin{bmatrix}\boldsymbol{C}\boldsymbol{x}_0+\boldsymbol{e}_0\\\boldsymbol{C}\bar{\boldsymbol{A}}\boldsymbol{x}_0+\boldsymbol{e}_1\\\vdots\\\boldsymbol{C}\bar{\boldsymbol{A}}^{T-1}\boldsymbol{x}_0+\boldsymbol{e}_{T-1}\end{bmatrix}\\=&\begin{bmatrix}\boldsymbol{C}\\\boldsymbol{C}\bar{\boldsymbol{A}}\\\vdots\\\boldsymbol{C}\bar{\boldsymbol{A}}^{T-1}\end{bmatrix}\boldsymbol{x}_0+\boldsymbol{E}_{q,\,T}:=\boldsymbol{\Phi}\boldsymbol{x}_0+\boldsymbol{E}_{q,\,T}\end{aligned} \tag{4}$$

其中, $\boldsymbol{Y}\in\mathbf{R}^{pT}$ 表示过去 T 时刻的堆叠量测向量, $\boldsymbol{\Phi}\in\mathbf{R}^{pT\times n}$ 表示闭环系统的观测性矩阵, 且有 $\mathrm{rank}\,(\boldsymbol{\Phi})=n$. 由命题 1 可知, 安全估计的目的是筛选最小的量测攻击通道集合. 因此, 通过堆叠量测方程使得安全估计问题转为稀疏优化或凸优化问题成为可能.

为确定可修复的受攻击通道最大数量, 给出如下命题, 通过判断闭环系统特征关系, 得到单一传感器节点可以接受的最大受攻击通道数.

命题 2[16]. 若 $\bar{\boldsymbol{A}}\in\mathbf{R}^{n\times n}$ 包含 n 个互异正特征值, 即 $0<\lambda_1<\lambda_2<\cdots<\lambda_n$, 且存在满秩矩阵 $\boldsymbol{C}\in\mathbf{R}^{p\times n}$ 使 $(\bar{\boldsymbol{A}},\,\boldsymbol{C})$ 可观测, 则存在有限时间 T, 使以下命题等价.

i) 存在状态估计器 $\mathcal{D}$ 在有限时间 T 内抵挡 q 个量测通道攻击;

ii) 对 $\bar{\boldsymbol{A}}$ 任意特征向量 $\boldsymbol{v}_j\in\mathbf{R}^n\,(j\in n)$, $|\mathrm{supp}\,(\boldsymbol{C}\boldsymbol{v}_j)|>2q$;

iii) 对 $\bar{\boldsymbol{A}}$ 任意特征向量 $\boldsymbol{v}_j\in\mathbf{R}^n\,(j\in n)$, $|\mathrm{supp}\,(\boldsymbol{\Phi}\boldsymbol{v}_j)|>2qT$;

iv) $\forall\boldsymbol{z}\in\mathbf{R}^n\backslash 0$, $|\mathrm{supp}\,(\boldsymbol{\Phi}\boldsymbol{z})|>2qT$.

若 $\boldsymbol{x}_0$ 已知, 则在压缩感知领域, 式 (4) 可等效为以下关于误差堆叠向量的稀疏误差修正问题[21], 其中 $\boldsymbol{b}\in\mathbf{R}^m$ 为量测向量, $\boldsymbol{A}\in\mathbf{R}^{m\times n}\,(m\ll n)$ 为感知矩阵. 引理 1 给出式 (5) 存在唯一解的充分条件.

$$\min_{\boldsymbol{x}}\|\boldsymbol{x}\|_{l_0},\ \ \boldsymbol{b}=\boldsymbol{A}\boldsymbol{x} \tag{5}$$

引理 1[22]. 若 $\boldsymbol{A}$ 的所有 $2q$ 个列向量均线性无关, 且 $m\ge 2q$, 则式 (5) 存在唯一的 q-稀疏解.

2　基于稀疏优化的安全估计

对于单一传感器节点遭受恶意量测攻击的目标

状态估计问题, 若采用卡尔曼滤波, 则首先应对恶意攻击信号进行还原和预测, 进而在量测更新方程中抵消其影响. 类似稀疏误差修正问题, 对于式 (4) 中的量测攻击信号, 给出如下结论.

定理 1. 给定 $\boldsymbol{Y}=\boldsymbol{\Phi z}+\boldsymbol{E}$, $\boldsymbol{\Phi}\in\mathbf{R}^{pT\times n}$ 为满秩矩阵, 且 $2s=2qT\leq pT-n$, 则以下命题等价.

i) 存在 QR 分解 $\boldsymbol{\Phi}=\begin{bmatrix}\boldsymbol{Q}_1 & \boldsymbol{Q}_2\end{bmatrix}\begin{bmatrix}\boldsymbol{R}_1\\ \boldsymbol{0}\end{bmatrix}$, 使矩阵 $\boldsymbol{Q}_2^{\mathrm{T}}\in\mathbf{R}^{(pT-n)\times pT}$ 的任意 $2s$ 个列向量线性无关;

ii) $\forall\boldsymbol{z}\in\mathbf{R}^n\backslash 0$, $|\mathrm{supp}\,(\boldsymbol{\Phi z})|>2s$.

证明. 设条件 ii) 成立, 若 $\boldsymbol{Q}_2^{\mathrm{T}}$ 存在 $2s$ 个列线性相关, 则存在 $\boldsymbol{E}_0\neq\boldsymbol{0}$ 使 $\boldsymbol{Q}_2^{\mathrm{T}}\boldsymbol{E}_0=\boldsymbol{0}$ 且 $|\mathrm{supp}\,(\boldsymbol{E}_0)|\leq 2s$. 由 $\boldsymbol{Q}_2^{\mathrm{T}}\boldsymbol{\Phi}=\boldsymbol{Q}_2^{\mathrm{T}}\boldsymbol{Q}_1\boldsymbol{R}_1=\boldsymbol{0}$, 易得 $\mathcal{N}\left(\boldsymbol{Q}_2^{\mathrm{T}}\right)=\mathcal{R}\left(\boldsymbol{\Phi}\right)$. 故 $\boldsymbol{E}_0\in\mathcal{R}\left(\boldsymbol{\Phi}\right)$, 即存在 $\boldsymbol{z}$ 使 $\boldsymbol{E}_0=\boldsymbol{\Phi z}$. 由于 $|\mathrm{supp}\,(\boldsymbol{E}_0)|=|\mathrm{supp}\,(\boldsymbol{\Phi z})|\leq 2s$ 与条件 ii) 相悖, 故 ii) $\Rightarrow$ i) 成立.

设条件 i) 成立, 若存在 $\boldsymbol{z}\in\mathbf{R}^n\backslash 0$ 使 $|\mathrm{supp}\,(\boldsymbol{\Phi z})|\leq 2s$, 则存在 L_1、L_2 为 $\{1,\cdots,pT\}$ 中两个不相交的子集, 且有 $|L_1|\leq s$, $|L_2|\leq s$, $L_1\oplus L_2=\mathrm{supp}\,(\boldsymbol{\Phi z})$. 令 $\boldsymbol{E}_1=\boldsymbol{\Phi z}\,|_{L_1}$ 表示使 $\boldsymbol{\Phi z}$ 非 L_1 项全为零的稀疏向量, 类似地定义稀疏向量 $\boldsymbol{E}_2=\boldsymbol{\Phi z}\,|_{L_2}$, 则 $\boldsymbol{\Phi z}=\boldsymbol{E}_1+\boldsymbol{E}_2$, 因此

$$\begin{aligned}\boldsymbol{Q}_2^{\mathrm{T}}\boldsymbol{Y}&=\boldsymbol{Q}_2^{\mathrm{T}}\left(\boldsymbol{\Phi z}+\boldsymbol{E}\right)=\\ &\quad\boldsymbol{Q}_2^{\mathrm{T}}\boldsymbol{E}=\\ &\quad\boldsymbol{Q}_2^{\mathrm{T}}\left(\boldsymbol{E}_1+\boldsymbol{E}_2+\boldsymbol{E}\right)\Rightarrow\\ \boldsymbol{Q}_2^{\mathrm{T}}&\left(\boldsymbol{E}_1+\boldsymbol{E}_2\right)=\boldsymbol{0}\end{aligned}$$

由于 $\boldsymbol{Q}_2^{\mathrm{T}}$ 中任意 $2s$ 个列向量线性无关, 因此 $\boldsymbol{E}_1+\boldsymbol{E}_2=\boldsymbol{0}$ 与假设相悖, 故 i)$\Rightarrow$ ii) 成立. □

推论 1. 给定如式 (4) 定义的量测堆叠方程, 且 $2qT\leq pT-n$. 设 $\bar{\boldsymbol{A}}\in\mathbf{R}^{n\times n}$ 包含 n 个互异正特征值, 其特征向量 $\boldsymbol{v}_j\in\mathbf{R}^n\,(j\in n)$ 有 $|\mathrm{supp}\,(\boldsymbol{C}\boldsymbol{v}_j)|>2q$, 且存在满秩矩阵 $\boldsymbol{C}\in\mathbf{R}^{p\times n}$ 使 $\left(\bar{\boldsymbol{A}},\,\boldsymbol{C}\right)$ 可观测. 若在有限时间 T 内至多存在 q 个量测通道攻击, 则如下问题有唯一解.

$$\begin{aligned}&\min_{\hat{\boldsymbol{E}}_{q,T}\in\mathbf{R}^{pT}}\left\|\hat{\boldsymbol{E}}_{q,T}\right\|_{l_0}\\ &\text{s.t. }\tilde{\boldsymbol{Y}}=\boldsymbol{Q}_2^{\mathrm{T}}\hat{\boldsymbol{E}}_{q,T},\ \left|\mathrm{supp}\left(\hat{\boldsymbol{E}}_{q,T}\right)\right|\leq qT\end{aligned}\tag{6}$$

其中, $\tilde{\boldsymbol{Y}}:=\boldsymbol{Q}_2^{\mathrm{T}}\boldsymbol{Y}$, $\boldsymbol{Q}_2$ 满足 QR 分解

$$\boldsymbol{\Phi}=\begin{bmatrix}\boldsymbol{Q}_1 & \boldsymbol{Q}_2\end{bmatrix}\begin{bmatrix}\boldsymbol{R}_1\\ \boldsymbol{0}\end{bmatrix}$$

证明. 由命题 2 及定理 1 可知, $\boldsymbol{Q}_2^{\mathrm{T}}$ 任意 $2s$ 个列向量线性无关, 根据引理 1 可知式 (6) 存在唯一解 $\boldsymbol{E}_{q,T}^*$ 且满足 $\left|\mathrm{supp}\left(\boldsymbol{E}_{q,T}^*\right)\right|\leq s$. □

推论 1 表明, 在闭环系统满足一定观测条件的基础上, 可通过求解 l_0 范数最小化还原量测攻击信号, 进而将安全估计问题转为稀疏优化问题. 为便于求解, 传统方法常用 l_1 范数[15−16] 近似替代 l_0 范数, 进而采用凸优化方法求解. 然而, 由于凸优化方法常采用启发式结构, 致使算法极易陷入局部最优, 在较短时限内不易收敛到精确解. 而问题本身存在的稀疏性特点也易使凸优化算法在正常通道可能求出不期望的干扰信号, 从而降低解算质量. 本文考虑以上凸优化问题弊端, 采用正交匹配追踪法[23] 直接求解 l_0 范数, 以保证解的稀疏性从而逼近真实攻击信号. 正交匹配追踪法通过贪婪迭代选择字典矩阵 $\boldsymbol{Q}_2^{\mathrm{T}}$ 的列, 使得在每次迭代过程中所选择的列与当前所得残差最大程度相关. 从原始信号中减去相关部分并反复迭代至达到预定稀疏度 $s=qT$ 为止. 通过求解式 (6) 得到过去 T 时刻的量测攻击信号预测值, 因此, 在卡尔曼滤波量测更新计算中抵消当前时刻的攻击信号, 可得到量测攻击下的单一传感器节点目标跟踪状态估计.

3 分布式稀疏优化安全估计

在弱量测攻击情况下 (如低幅值高斯白噪声), 采用 OMP 及稀疏优化能够提供单一传感器节点较好的安全估计精度. 然而, 在 FDI 等复杂攻击条件下, 由于 OMP 在每次过程迭代中仅选取一个原子来更新支撑集, 导致要获得足够精度的状态估计需要付出较高的时间代价, 影响实时性[24]. 在实际情况中, 受限于发射功率与作用距离, 攻击者在每时刻仅能对 DSN 中的若干节点实施针对性攻击, 而对多数节点则采取弱干扰形式. 这就为构建高置信度的分布式安全状态估计方法, 利用 DSN 多节点之间的信息交互提升目标状态跟踪稳定性创造了可能. 本节在上节稀疏优化理论基础上, 进一步考虑多节点协同方式, 给出一种基于势博弈理论的分布式安全状态估计架构, 通过邻域节点共享信息, 提供一种简洁可靠的节点选择与数据融合机制, 以提升 DSN 在复杂攻击条件下的整体网络状态跟踪可靠性.

3.1 势博弈原理

势博弈[25−26] 是控制多智能体系统协调一致的主要方法之一, 被广泛用于网络化集群与分布式系统中. 势博弈可用一个三元组 $\mathcal{G}=\langle\mathcal{P},\,\mathcal{A},\,\mathcal{U}\rangle$ 表示, 其中 $\mathcal{P}=\{1,\cdots,N\}$ 表示博弈参与者集合, 这里代表 DSN 的节点集合; $\mathcal{A}=\{a_i,\,i\in\mathcal{P}\}$ 表示策略集, 其中 a_i 表示节点 i 的可选策略, 用 $A_i=\{a_i,\,a_{-i}\}\in\mathcal{A}$ 表示节点 i 选择策略 a_i 且其他节点选择策略 a_{-i} 时

的策略组合; $\mathcal{U}=\{U_i: A_i\to\mathbf{R},\ i\in\mathcal{P}\}$ 代表节点的效用函数集合, 其中 $U_i\left(a_i,\ a_{-i}\right)$ 为节点 i 选择策略组合 A_i 时的收益.

定义 2[25]. 给定势博弈 $\mathcal{G}=\langle\mathcal{P},\ \mathcal{A},\ \mathcal{U}\rangle$, 若存在策略组合 $A^*=\left\{a_i^*,\ a_{-i}^*\right\}$, 使下式成立

$$U_i\left(a_i^*,\ a_{-i}^*\right)\geq U_i\left(a_i,\ a_{-i}^*\right),\ \ \forall i\in\mathcal{P},\ \ a_i\in\mathcal{A}$$

则 A^* 为势博弈 $\mathcal{G}$ 的一个纳什均衡.

定义 3[26]. 给定势博弈 $\mathcal{G}=\langle\mathcal{P},\ \mathcal{A},\ \mathcal{U}\rangle$, 若存在函数 $V:\mathcal{A}\to\mathbf{R}$, 使下式成立

$$\begin{aligned}&U_i\left(a'_i,\ a_{-i}\right)-U_i\left(a_i,\ a_{-i}\right)=\\&V\left(a'_i,\ a_{-i}\right)-V\left(a_i,\ a_{-i}\right)\\&\forall i\in\mathcal{P},\ \ \forall a_i,\ a'_i,\ a_{-i}\in\mathcal{A}\end{aligned}$$

则称 $\mathcal{G}$ 为精准势博弈, V 为势函数, 精准势博弈必然存在一个纳什均衡.

3.2　基于势博弈的分布式稀疏优化安全估计

对于 DSN 而言, 由于不同节点受到的攻击程度不同, 多数节点通过稀疏优化能够获得较为精确的目标跟踪状态估计, 而遭受复杂干扰的节点需要依靠邻域信息获得稳定的安全状态估计值. 本节采用势博弈理论进行分布式稀疏优化安全估计, 即在 DSN 中寻找纳什均衡策略使 DSN 整体的目标跟踪效果达到最优.

对于节点 $i\in\{1,\cdots,\ N\}$, 设计以下效用函数 $U_i\left(a_i,\ a_{-i}\right)$:

$$\begin{aligned}U_i=&-r\ln\left(\max\left(\boldsymbol{E}_{q,T}^{(i)}\right)\right)-\\&\sum_{j\in N_i}\left\|\mathrm{xor}\left(\mathrm{sgn}\left(\boldsymbol{E}_{q,T}^{(i)}\right),\ \mathrm{sgn}\left(\boldsymbol{E}_{q,T}^{(j)}\right)\right)\right\|\end{aligned}\tag{7}$$

其中, $\boldsymbol{E}_{q,T}^{(i)}$ 表示节点 i 在过去 T 时刻的量测误差估计值; N_i 表示节点 i 的邻居集合, 由通信拓扑结构决定; sgn 为二进制符号函数, 其定义如下

$$\mathrm{sgn}\left(x\right)=\begin{cases}1, & x\neq 0\\ 0, & x=0\end{cases}\tag{8}$$

函数 $\mathrm{xor}\left(a,b\right)$ 表示两个二进制序列 a 和 b 的异或运算, 其输出向量用于统计 a 和 b 的二进制编码差异性; $r>0$ 为惩罚因子. 节点 i 的可选策略定义为由邻域状态估计组成的三元组 $a_i\in\Theta_i:=\left\{\left\langle\bar{\boldsymbol{x}}_{k+1}^{(j)},\boldsymbol{P}_{k+1}^{(j)},\boldsymbol{E}_{q,T}^{(j)}\right\rangle|j\in N_i\cup i\right\}$, 其中, $\bar{\boldsymbol{x}}_{k+1}^{(j)}$ 和 $\boldsymbol{P}_{k+1}^{(j)}$ 分别为节点 j 通过卡尔曼滤波输出的下一时刻目标状态观测值及误差协方差矩阵. 式 (7) 的意义在于, 每个传感器节点预估的堆叠误差向量 $\boldsymbol{E}_{q,T}$ 总是具有 s-稀疏结构, 通过异或操作能够检测出该节点的误差向量与其他相邻节点误差向量的差异性. 由于 DSN 中多数节点受攻击强度较弱, 对于可靠节点而言, 其堆叠误差向量稀疏结构应与多数相邻节点一致, 存在显著差异的则需降低其效用收益, 在后续策略选择时给予较低的选择概率. 此外, 对于噪声幅度较小的误差信号则应提高其收益值, 进而获得更高的选择概率.

注 3. 对于式 (7) 的效用函数, 还可以设计参考稀疏向量, 通过异或操作对比堆叠误差向量与参考稀疏向量的结构差异性以筛选有效节点策略. 例如, 采用文献 [8] 中的参考矢量构造法, 并经过稀疏映射[17−18] 后生成参考稀疏向量.

给定势函数 $V=\sum_{i=1}^{N}U_i\left(a_i,\ a_{-i}\right)$, 由于效用函数 U_i 仅与当前时刻的决策集有关, 且不受其他节点影响, 则有

$$\begin{aligned}&V\left(a'_i,\ a_{-i}\right)-V\left(a_i,\ a_{-i}\right)=\\&U_i\left(a'_i,\ a_{-i}\right)-U_i\left(a_i,\ a_{-i}\right)+\\&\sum_{k\neq i}U_k\left(a_k,\ a_{-k}\right)-\sum_{k\neq i}U_k\left(a_k,\ a_{-k}\right)=\\&U_i\left(a'_i,\ a_{-i}\right)-U_i\left(a_i,\ a_{-i}\right)\end{aligned}$$

显然 $V\left(a_i,\ a_{-i}\right)$ 符合精准势博弈, 采用式 (7) 的效用函数必定存在纳什均衡. 节点 i 的策略选择方式采用如下概率学习方式[25]

$$\Pi_i\left(a_i\right)=\frac{\exp\left\{\beta U_i\left(a_i,\ a_{-i}\right)\right\}}{\sum\limits_{a'_i\in\Theta_i}\exp\left\{\beta U_i\left(a'_i,\ a_{-i}\right)\right\}}\tag{9}$$

其中, $\Pi_i\left(a_i\right)$ 表示节点 i 选择策略 a_i 的概率, $\beta>0$ 为学习因子. 完成策略选择后, 节点 i 将所选策略 a_i 中的状态估计值与误差协方差矩阵对应替换当前时刻计算的卡尔曼滤波输出结果 $\bar{\boldsymbol{x}}_{k+1}^{(j)}$ 与 $\boldsymbol{P}_{k+1}^{(j)}$, 从而获得更为可靠的安全状态估计. 图 1 给出了基于势博弈的分布式稀疏优化安全状态估计计算流程.

4　仿真分析

本节给出一个典型应用实例, 验证所提方法的有效性. 该实例采用 5 部地面探测装置对一个三维目标运动进行状态跟踪, 地面探测装置组网构成一套 DSN 地面探测系统. 每部装置采用雷达获取与目标的相对距离、方位和俯仰角, 此外还可通过视觉、红外等测量方式获取目标在笛卡尔坐标系下的三维速度. 攻击者会在不同时段针对雷达的测距和方位测量通道实施几类量测攻击, 通过对比仿真验证本文方法的有效性.

设目标状态由其三维位置 $\{p_x,\ p_y,\ p_z\}$ 和三维速度 $\{v_x,\ v_y,\ v_z\}$ 表示, 即

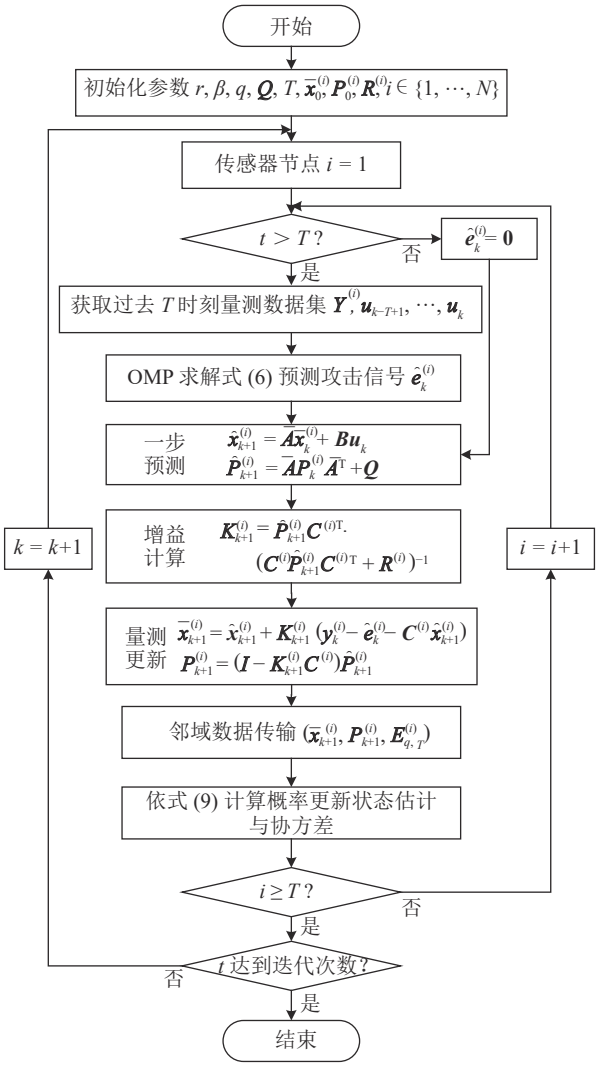


图 1 分布式稀疏优化安全状态估计流程图

Fig. 1 Flowchart of secure state estimation algorithm based on distributed sparse optimizations

$$\boldsymbol{x} = [p_x,\ v_x,\ p_y,\ v_y,\ p_z,\ v_z]^{\mathrm{T}}$$

目标控制量 $\boldsymbol{u}$ 为其三维加速度, 则运动模型满足以下系统矩阵

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_{11} & & \\ & \boldsymbol{A}_{22} & \\ & & \boldsymbol{A}_{33} \end{bmatrix}$$

$$\boldsymbol{A}_{11} = \boldsymbol{A}_{22} = \boldsymbol{A}_{33} = \begin{bmatrix} 1 & T_s \\ 0 & 1 \end{bmatrix}$$

$$\boldsymbol{B} = \begin{bmatrix} T_s^2/2 & T_s & 0 & 0 & 0 & 0 \\ 0 & 0 & T_s^2/2 & T_s & 0 & 0 \\ 0 & 0 & 0 & 0 & T_s^2/2 & T_s \end{bmatrix}^{\mathrm{T}}$$

其中, $T_s = 0.05$ 表示时间步长. 设目标采用状态反馈 $\boldsymbol{u}_k = \boldsymbol{G}\boldsymbol{x}_k$ 将闭环系统极点配置为 $0.99 \pm 0.01\mathrm{i}$、$0.98 \pm 0.02\mathrm{i}$ 、$0.97 \pm 0.03\mathrm{i}$ 以满足推论 1 的充分条件. 对于探测装置量测模型, 可建立以下量测矢量

$$\boldsymbol{y}^{(i)} = \left[\rho^{(i)},\ \psi^{(i)},\ \theta^{(i)},\ v_x,\ v_y,\ v_z\right]^{\mathrm{T}}$$

其中, $\{\rho^{(i)},\ \psi^{(i)},\ \theta^{(i)}\}$ 分别表示第 i 部探测装置相对目标当前位置的径向距离、方位和俯仰角. 设第 i 部装置位于 $\left\{\breve{p}_x^{(i)},\ \breve{p}_y^{(i)},\ \breve{p}_z^{(i)}\right\}$, 则有

$$\rho^{(i)} = \sqrt{\Delta p_x^2 + \Delta p_y^2 + \Delta p_z^2}$$
$$\psi^{(i)} = \arctan\left(\Delta p_y / \Delta p_x\right)$$
$$\theta^{(i)} = \arctan\left(\Delta p_z / \rho_2^{(i)}\right),\ \rho_2^{(i)} = \sqrt{\Delta p_x^2 + \Delta p_y^2}$$
$$\Delta p_x = p_x - \breve{p}_x^{(i)},\ \Delta p_y = p_y - \breve{p}_y^{(i)},\ \Delta p_z = p_z - \breve{p}_z^{(i)}$$

显然, 量测矢量中存在目标状态的非线性函数, 若要应用所提方法需转为线性模型. 令

$$\bar{\boldsymbol{x}}_k^{(i)} = \left[\bar{p}_x^{(i)},\ \bar{v}_x^{(i)},\ \bar{p}_y^{(i)},\ \bar{v}_y^{(i)},\ \bar{p}_z^{(i)},\ \bar{v}_z^{(i)}\right]^{\mathrm{T}}$$

表示第 i 部装置在当前时刻的目标状态估计值. 类似扩展卡尔曼滤波, 将量测矢量非线性项在 $\bar{\boldsymbol{x}}_k^{(i)}$ 处取一阶泰勒展开, 得到

$$\boldsymbol{y}_k^{(i)} = \boldsymbol{C}^{(i)}\left(\boldsymbol{x}_k - \breve{\boldsymbol{x}}_k^{(i)}\right) + \boldsymbol{e}_k^{(i)} + \boldsymbol{v}_k^{(i)}$$

$$\boldsymbol{C}^{(i)} = \begin{bmatrix} \dfrac{\Delta\bar{p}_x^{(i)}}{\bar{\rho}^{(i)}} & 0 & \dfrac{\Delta\bar{p}_y^{(i)}}{\bar{\rho}^{(i)}} & 0 & \dfrac{\Delta\bar{p}_z^{(i)}}{\bar{\rho}^{(i)}} & 0 \\ \dfrac{-\Delta\bar{p}_y^{(i)}}{\bar{\rho}_2^{(i)}} & 0 & \dfrac{\Delta\bar{p}_x^{(i)}}{\bar{\rho}_2^{(i)}} & 0 & 0 & 0 \\ \dfrac{-\Delta\bar{p}_x^{(i)}\Delta\bar{p}_z^{(i)}}{\bar{\rho}_2^{(i)}\bar{\rho}^{(i)2}} & 0 & \dfrac{-\Delta\bar{p}_y^{(i)}\Delta\bar{p}_z^{(i)}}{\bar{\rho}_2^{(i)}\bar{\rho}^{(i)2}} & 0 & \dfrac{\rho_2^{(i)2}}{\bar{\rho}^{(i)2}} & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\Delta\bar{p}_x = \bar{p}_x^{(i)} - \breve{p}_x^{(i)},\ \Delta\bar{p}_y = \bar{p}_y^{(i)} - \breve{p}_y^{(i)},\ \Delta\bar{p}_z = \bar{p}_z^{(i)} - \breve{p}_z^{(i)}$$

$$\bar{\rho}^{(i)} = \sqrt{\Delta\bar{p}_x^2 + \Delta\bar{p}_y^2 + \Delta\bar{p}_z^2},\ \bar{\rho}_2^{(i)} = \sqrt{\Delta\bar{p}_x^2 + \Delta\bar{p}_y^2}$$

其中, $\breve{\boldsymbol{x}}_k^{(i)} = \left[\breve{p}_x^{(i)},\ 0,\ \breve{p}_y^{(i)},\ 0,\ \breve{p}_z^{(i)},\ 0\right]^{\mathrm{T}}$ 为第 i 部装置固定状态. 尽管量测矩阵为时变矩阵, 通过分析可知 $(\bar{\boldsymbol{A}},\ \boldsymbol{C})$ 仍可构成可观测对. 设目标初始状态为 $\boldsymbol{x}_0 = [10,\ 0,\ 10,\ 0,\ 8,\ 0]^{\mathrm{T}}$, 误差协方差矩阵为 $\boldsymbol{P}_0 = 0.1^2\boldsymbol{I}_6$, 高斯白噪声统计特性服从 $\boldsymbol{Q} = 0.005^2\boldsymbol{I}_6$、$\boldsymbol{R} = 0.01^2\boldsymbol{I}_6$. 量测攻击信号为针对雷达测距和方位的分时段攻击, 共两种攻击模式, 每种攻击模式下的攻击矢量

描述如下

$$\text{I类}: \boldsymbol{e}_k^{(i)} \sim [\mathrm{U}(-5,\ 5),\ \mathrm{U}(0,\ 2\pi),\ 0,\ 0,\ 0,\ 0]^{\mathrm{T}}$$

$$\text{II类}: \boldsymbol{e}_k^{(i)} \sim \left[\mathrm{U}(-5,\ 5)+10,\ \tilde{\psi},\ 0,\ 0,\ 0,\ 0\right]^{\mathrm{T}}$$

其中, $\mathrm{U}(a,\ b)$ 表示区间 $(a,\ b)$ 内均匀分布, $\tilde{\psi}$ 为区间 $(0,\ 2\pi)$ 内的定值, 每部装置遭受的分时段攻击情况如表 1 所示. DSN 通信拓扑结构由图 2 给出, 设所有探测节点的初始估计状态与 $\boldsymbol{x}_0$ 一致, 将所提算法分别与 4 种当下流行的安全估计或分布式状态估计算法进行对比测试, 以验证其可靠性.

表 1　DSN 遭受的分时段攻击列表

Table 1　Time sharing attacks of DSN detection nodes

节点	时段			
	0 s ~ 3 s	3 s ~ 6 s	6 s ~ 9 s	9 s ~ 10 s
1	无	无	无	I类
2	I类	I类	无	无
3	无	无	II类	II类
4	II类	II类	无	无
5	无	无	I类	I类

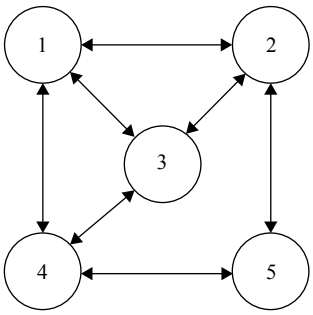


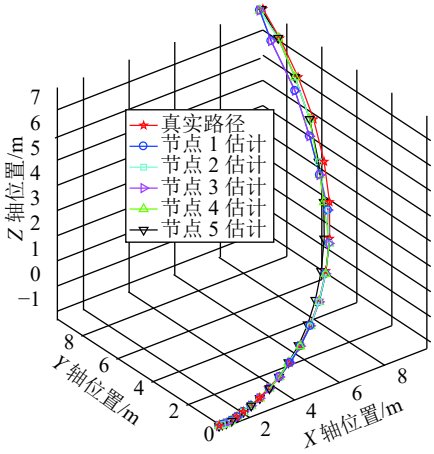
图 2　DSN 网络通信拓扑结构

Fig. 2　Communication topology of DSN nodes

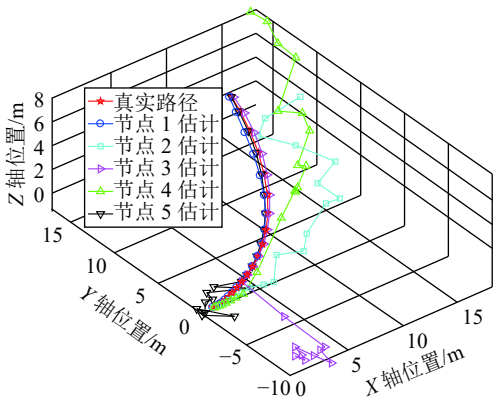
对比仿真中每种算法定义如下: A1) 基于势博弈的分布式稀疏优化安全估计, 其初始参数配置为 $r=2$, $\beta=10$, $q=2$, $T=6$; A2) 基于 l_1 范数的凸优化安全估计, 即采用 l_1 范数取代 l_0 范数对误差进行求解, 凸优化算法采用对偶内点法 (Primal-dual interior-point algorithm, PDIPA)[27]; A3) 分布式卡尔曼滤波[28](Distributed Kalman filter, DKF); A4) 基于事件触发机制映射梯度法 (Event-triggered projected gradient, ETPG)[17], 其作用原理为采用一种稀疏映射方式求解基于 SBO 问题的稀疏攻击信号序列; A5) S-dLMS 算法, 通过分布式处理识别 DSN 中的受攻击节点, 从而进行可靠目标状态数据融合. 下面给出仿真结果.

图 3 给出各种对比方法对目标运动轨迹的跟踪结果. 可见, 分布式稀疏优化估计方法相比其他方法具有更好的精确度. 基于 l_1 范数最小化的凸优化安全估计方法虽然在理论上能够还原量测攻击信号, 然而实际应用中难以精确求解. 图 4 给出了各种测试算法对目标横向位置的跟踪误差变化情况. 从图 3、图 4 结果来看, 凸优化方法对 II 类攻击的还原能力尤其偏弱, 而 II 类攻击可看成是一种复合攻击模式, 即在 I 类随机噪声攻击模式基础上叠加固定偏量的攻击信号, 以模拟 FDI 信号的攻击特性. 在凸优化方法测试中, 探测节点 3、4 先后受到 II 类量测攻击导致其估计水平发生显著性降低, 而探测节点 2 在前期受到 I 类攻击影响, 表现同样不稳定, 表明该方法未能成功还原两类攻击信号. 其原因主要在于堆叠误差方程的高维度和稀疏性使其存在较多的局部最优解, 而凸优化方法采取启发式搜索策略虽然降低了计算复杂度但极易陷入局部最优. 此外, 图 5 仿真结果显示凸优化方法在速度通道检测出了一定的误差信号, 相当于在正常通道加入了不期望的攻击信号, 这对于系统状态估计同样有不良影响. 而分布式稀疏优化则在速度通道保持了较好的估计特性, 误检测概率较低. 由于利用了解的稀疏性, 使还原的攻击信号在正常通道有较大概率为零. 即使存在局部最优, 通过后续的势博弈协同机制也能够有很大概率检测和排除此类误解节点, 通过融合可靠节点数据依然可以获取精准的目标跟踪状态数据.

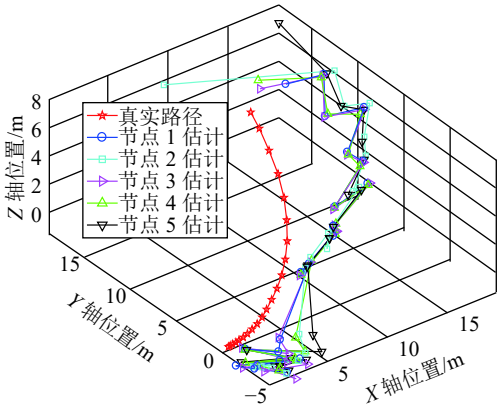
表 2 给出了 5 种算法对目标横向位置的均方估计误差. 根据表 2 显示结果, DKF 在所有节点的估计性能表现最差. DKF 可等效为一个集中式的卡尔曼滤波器, 仅考虑各节点的信息一致性, 而忽略了噪声攻击对节点量测过程的影响, 从而使其在处理量测攻击的问题上不具备优势. ETPG 在处理稀疏攻击问题中采取了与本文所提方法相似的方式, 即将堆叠方程映射为一种求解 s-稀疏攻击信号的安全估计问题, 采用映射梯度法求解稀疏攻击信号. 从仿真结果看出, ETPG 也出现了凸优化算法在 II 类攻击信号还原中的问题, 即陷入局部最优, 两种方法在检测受攻击通道时表现出了相似的性能. 但 ETPG 在正常通道未出现不期望的误解现象, 表明保留解的稀疏性对于安全估计的重要性. S-dLMS 则表现出较好的性能, 其在节点信息一致性方面甚至优于本文所提方法. 然而, 仿真结果表明 S-dLMS 出现了明显的稳态误差, 且随着时间推移, 误差有发散迹象. S-dLMS 在执行过程中通过节点之间共享局部量测新息, 利用中值排序获得参考估计向量, 通过比较相邻节点与参考向量的差异筛选可靠节点. 这种检测–融合的分布式机制极大增强了 S-dLMS 在处理 I 类随机噪声攻击及部分 FDI 攻击过程中的鲁棒性. 然而, 本节中的 II 类量测攻击信号由于



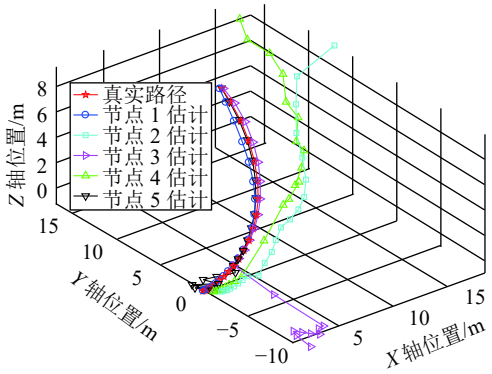
(a) A1 中 DSN 探测节点对目标轨迹的跟踪结果
(a) Target tracking by the DSN detection nodes of A1



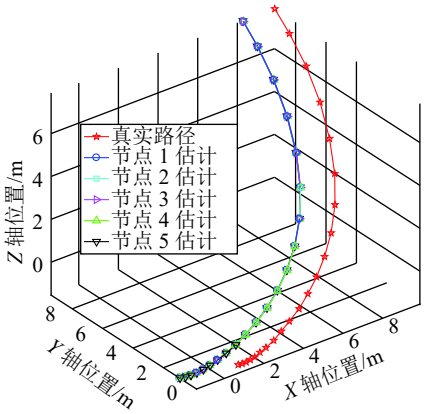
(b) A2 中 DSN 探测节点对目标轨迹的跟踪结果
(b) Target tracking by the DSN detection nodes of A2



(c) A3 中 DSN 探测节点对目标轨迹的跟踪结果
(c) Target tracking by the DSN detection nodes of A3



(d) A4 中 DSN 探测节点对目标轨迹的跟踪结果
(d) Target tracking by the DSN detection nodes of A4

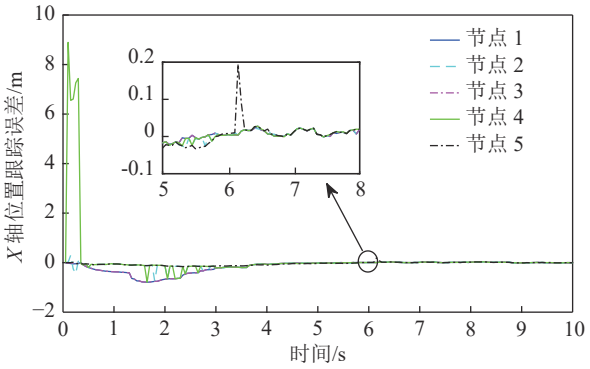


(e) A5 中 DSN 探测节点对目标轨迹的跟踪结果
(e) Target tracking by the DSN detection nodes of A5

图 3 测试算法对目标轨迹的跟踪效果对比

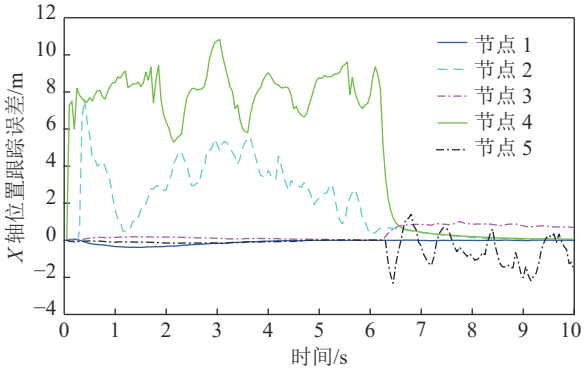
Fig. 3 Comparison of trajectory tracking by the candidate algorithms

出现了固定偏向量测误差, 使 S-dLMS 的中值排序可能检测出带有偏离信号的参考估计向量. 由于融合过程以参考向量为基准, 这就造成了稳态误差的出现. 相比之下, 本文所提方法在检测可靠节点处理中, 未采用参考向量而是基于节点之间的稀疏度近似与噪声大小, 这就避免了因参考向量处理不当



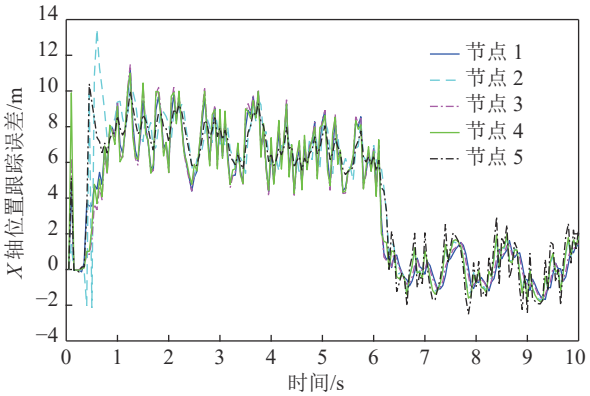
(a) A1 中各节点对目标 X 轴位置的跟踪误差

(a) Estimation errors of X positions by the DSN nodes of A1



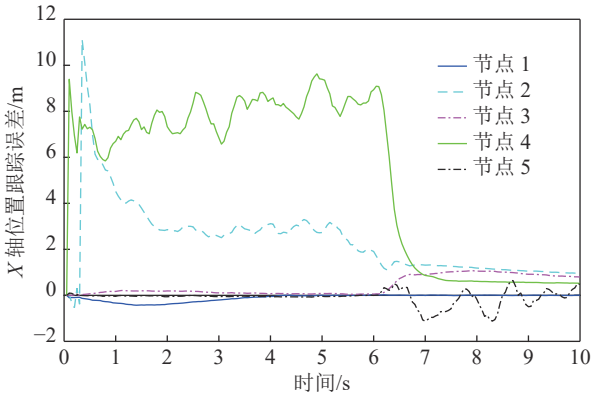
(b) A2 中各节点对目标 X 轴速度的跟踪误差

(b) Estimation errors of X positions by the DSN nodes of A2



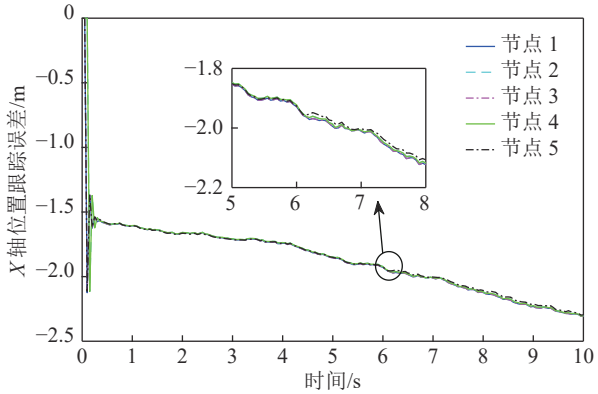
(c) A3 中各节点对目标 X 轴位置的跟踪误差

(c) Estimation errors of X positions by the DSN nodes of A3



(d) A4 中各节点对目标 X 轴位置的跟踪误差

(d) Estimation errors of X positions by the DSN nodes of A4



(e) A5 中各节点对目标 X 轴位置的跟踪误差

(e) Estimation errors of X positions by the DSN nodes of A5

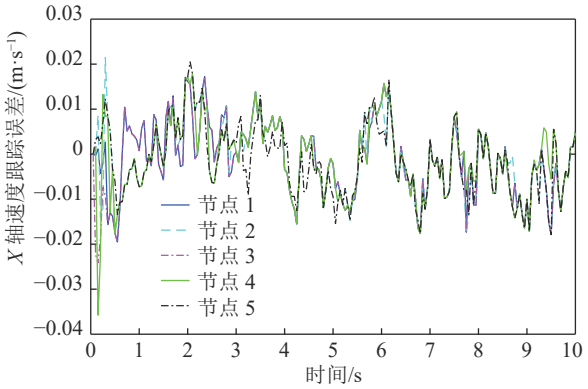
图 4　测试算法对目标 X 轴位置的跟踪误差对比

Fig. 4　Comparison of X-position estimation errors by the candidate algorithms

而可能出现的整体偏离. 当然, 若能将参考向量设计标准细化, 使其能够应对多种攻击模式, 则能进一步提升 S-dLMS 的效用.

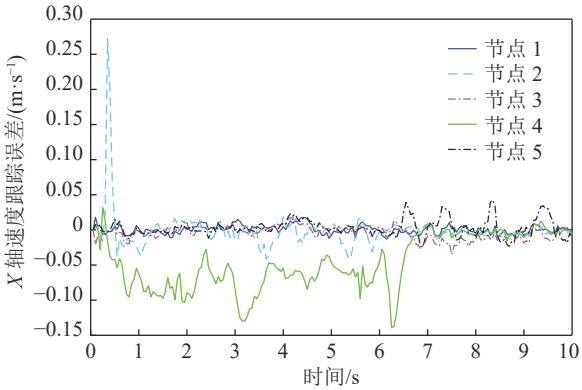
图 6 给出了所提方法通过势博弈机制为每个探测节点选择的融合策略变化情况, 融合节点序号表示选择的相邻探测节点编号. 可以看出, 在效用函数的协调下, 在不同时刻受到恶意攻击的探测节点会自动选择稀疏结构和噪声幅度更为合理的相邻节点状态估计数据, 进而避免陷入局部最优和出现显著估计误差. 当 DSN 规模逐步扩大, 其安全估计稳定性会随着可靠性节点的增多而进一步提升.

实际情况中, 恶意量测攻击信号也许会有多种模式, 每种模式差异显著, 在融合后无差别特性增强, 常规的 CPS 异常检测装置往往会被误导而不易发现. 在这种情况下, 对于所提方法, 一方面可通过扩大 DSN 节点规模, 保证正常节点的数量优势.



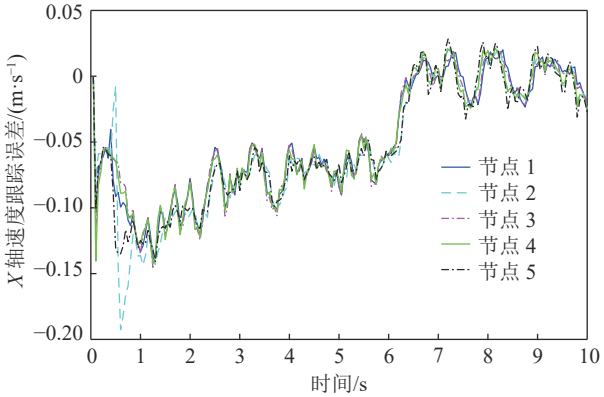
(a) A1 中各节点对目标 X 轴速度的跟踪误差

(a) Estimation errors of X velocities by the DSN nodes of A1



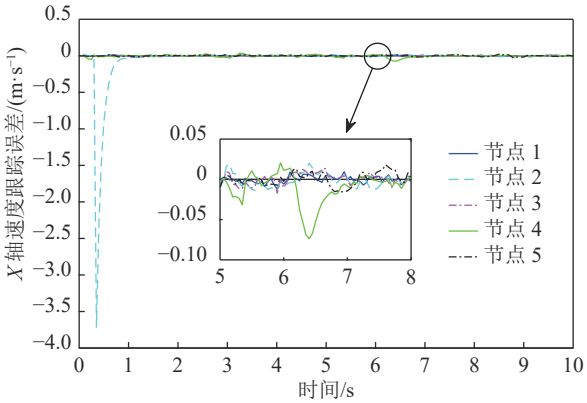
(b) A2 中各节点对目标 X 轴速度的跟踪误差

(b) Estimation errors of X velocities by the DSN nodes of A2



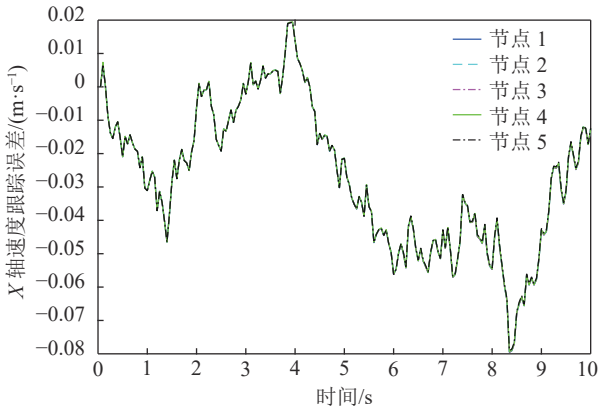
(c) A3 中各节点对目标 X 轴速度的跟踪误差

(c) Estimation errors of X velocities by the DSN nodes of A3



(d) A4 中各节点对目标 X 轴速度的跟踪误差

(d) Estimation errors of X velocities by the DSN nodes of A4



(e) A5 中各节点对目标 X 轴速度的跟踪误差

(e) Estimation errors of X velocities by the DSN nodes of A5

图 5 测试算法对目标 X 轴速度的跟踪误差对比

Fig. 5 Comparison of X-velocity estimation errors by the candidate algorithms

由于异常节点始终与正常节点存在量测数据差异 (如协方差、中值等统计特性), 因此利用势博弈机制可以较为容易地检测出异常节点, 从而在融合选择过程使用可靠性更高的节点估计状态, 保证系统鲁棒性. 另一方面, 可参考 S-dLMS 的处理方式, 构建两个子系统分别用于本地新息处理和全局融合处理, 两系统各自独立运行. 本地子系统通过分析本地量测数据统计特性判断是否出现异常, 若无法辨识量测攻击信号, 则将本地数据共享至全局网络, 在全局融合子系统中利用势博弈机制筛选满足正常统计特性的有效节点. 该方案对于网络连通性有较高要求, 当节点密度较大时, 其网络通信压力和计算复杂度会显著提升, 因此更适于作为安全估计的离线处理方案.

表 2　5 种算法对 X 轴位置的均方估计误差比较 (m)

Table 2　Comparison of mean square errors (meters) of position estimations in X-axis by the five algorithms

	A1	A2	A3	A4	A5
节点 1	0.0724	0.0238	28.6083	0.0302	3.6060
节点 2	0.0150	7.2185	33.0688	8.3714	3.5778
节点 3	0.0724	0.2550	29.0511	0.3338	3.6056
节点 4	1.3807	40.6553	29.5093	39.4624	3.5778
节点 5	0.0054	0.4213	31.6166	0.1078	3.5785

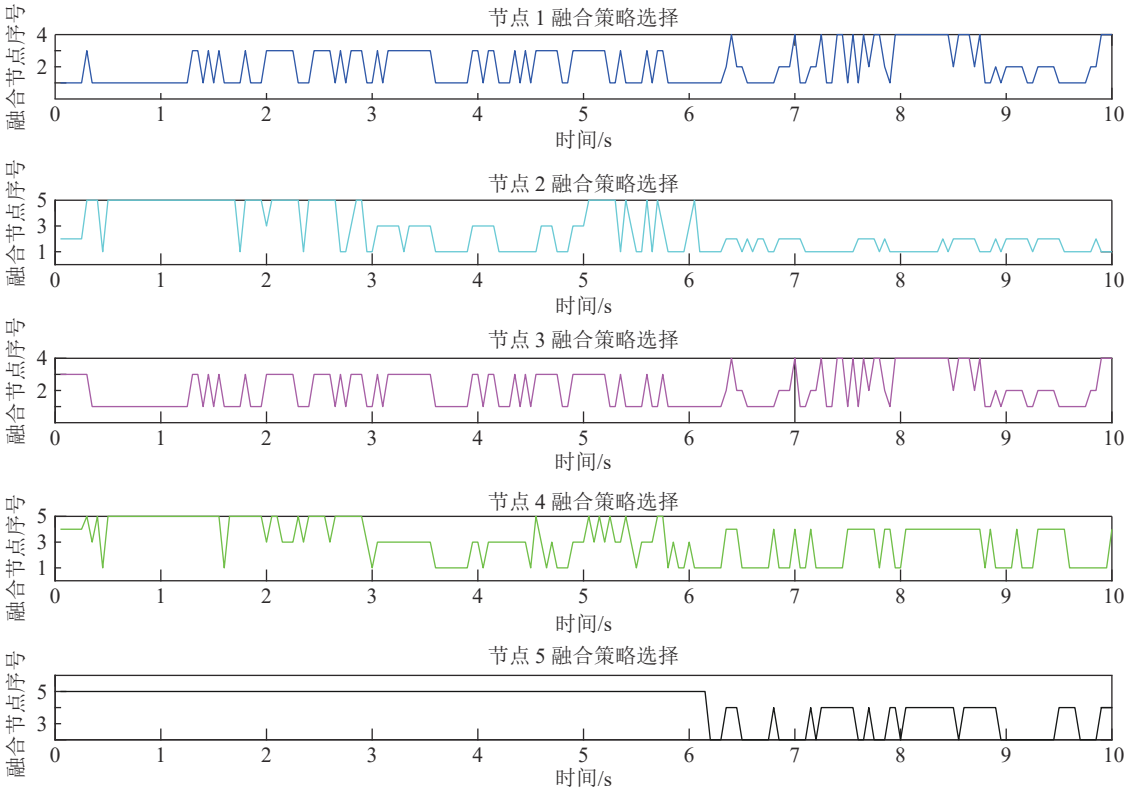


图 6　算法 A1 中探测节点的融合策略选择

Fig. 6　Fusion decision making by the nodes in A1

5　结论

针对恶意量测攻击下的分布式传感器网络目标状态跟踪问题, 提出一种分布式稀疏优化安全状态估计方法. 借鉴压缩感知原理, 将安全估计转为基于 l_0 范数的稀疏优化问题, 采用正交匹配追踪法重构未知攻击信号, 并结合卡尔曼滤波恢复跟踪目标的真实状态. 相比当下流行的凸优化攻击信号求解策略, 所提方法充分考虑了攻击信号的稀疏性特征, 借助于其特殊结构提高信号重构的求解质量. 对于恶意信号注入等复杂攻击模式, 考虑 DSN 分布式架构, 提出一种基于势博弈的分布式稀疏优化安全估计方法, 利用相邻 DSN 节点之间的信息交互实现可靠融合策略, 提升 DSN 整体的目标跟踪与状态估计稳定性. 对比仿真结果表明本文所提方法的有效性.

然而, 在实际应用中, DSN 信息交互过程仍然可能存在通信噪声甚至信道攻击. 通信干扰会显著影响分布式安全状态估计的处理过程. 此外, 现实情况中跟踪目标的运动模型同样存在很多不确定性. 因此, 考虑更为全面的实际环境特点, 是后续相关技术领域的研究重点.

References

1　Rajkumar R, Lee I, Sha L, Stankovic J. Cyber-physical systems: The next computing revolution. In: Proceedings of the 47th Design Automation Conference. Anaheim, CA, USA: IEEE, 2010. 731−736

2　Pang Yan, Wang Na, Xia Hao. A game theory approach for secure control of cyber-physical systems. *Acta Automatica Sinica*,

2019, **45**(1): 185−195
(庞岩, 王娜, 夏浩. 基于博弈论的信息物理融合系统安全控制. 自动化学报, 2019, **45**(1): 185−195)

3 Ding D, Han Q, Wang Z, Ge X. A survey on model-based distributed control and filtering for industrial cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 2019, **15**(5): 2483−2499

4 Torfs T, Sterken T, Brebels S, Santana J, Van Den Hoven R, Spiering V, et al. Low power wireless sensor network for building monitoring. *IEEE Sensors Journal*, 2013, **13**(3): 909−915

5 Gupta H P, Rao S V, Venkatesh T. Critical sensor density for partial coverage under border effects in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 2014, **13**(5): 2374−2382

6 Liu S, Chen B, Zourntos T, Kundur D, Butler-Purry K. A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Transactions on Smart Grid*, 2014, **5**(3): 1183−1195

7 Guan Y, Ge X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Transactions on Signal and Information Processing Over Networks*, 2018, **4**(1): 48−59

8 Liu Y, Li C. Secure distributed estimation over wireless sensor networks under attacks. *IEEE Transactions on Aerospace and Electronic Systems*, 2018, **54**(4): 1815−1831

9 Yuan Tian, Luo Zhen-Ming, Liu Chen, Che Wei. Antagonistic method of deception and noise complex jamming against netted radar. *Journal of Detection and Control*, 2019, **41**(6): 69−74
(袁天, 罗震明, 刘晨, 车伟. 基于欺骗噪声复合干扰的组网雷达对抗方法. 探测与控制学报, 2019, **41**(6): 69−74)

10 Cintuglu M H, Ishchenko D. Secure distributed state estimation for networked microgrids. *IEEE Internet of Things Journal*, 2019, **6**(5): 8046−8055

11 Manandhar K, Cao X, Hu F, Liu Y. Combating false data injection attacks in smart grid using Kalman filter. In: Proceedings of the 3rd International Conference on Computing, Networking and Communications. Honolulu, HI, USA: IEEE, 2014. 16−20

12 Li Y, Shi L, Cheng P, Chen J, Quevedo D E. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 2015, **60**(10): 2831−2836

13 Kwon C, Hwang I. Hybrid robust controller design: Cyber attack attenuation for cyber-physical systems. In: Proceedings of the 52nd IEEE Conference on Decision and Control. Florence, Italy: IEEE, 2013. 188−193

14 Zhou Xue, Zhang Hao, Wang Zhu-Ping. Extended Kalman filtering in state estimation systems with malicious attacks. *Acta Automatica Sinica*, 2020, **46**(1): 38−46
(周雪, 张皓, 王祝萍. 扩展卡尔曼滤波在受到恶意攻击系统中的状态估计. 自动化学报, 2020, **46**(1): 38−46)

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

16 Chang Y H, Hu Q, Tomlin C J. Secure estimation based Kalman filter for cyber-physical systems against sensor attacks. *Automatica*, 2018, **95**: 399−412

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

18 Wu C, Hu Z, Liu J, Wu L. Secure estimation for cyber-physical systems via sliding mode. *IEEE Transactions on Cybernetics*, 2018, **48**(12): 3420−3431

19 Liang C, Wen F, Wang Z. Trust-based distributed Kalman filtering for target tracking under malicious cyber attacks. *Information Fusion*, 2019, **46**: 44−50

20 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
(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)

21 Candes E J, Tao T. Decoding by linear programming. *IEEE Transactions on Information Theory*, 2005, **51**(12): 4203−4215

22 Hayden D, Chang Y H, Goncalves J, Tomlin C J. Sparse network identifiability via compressed sensing. *Automatica*, 2016, **68**: 9−17

23 Cai T T, Wang L. Orthogonal matching pursuit for sparse signal recovery with noise. *IEEE Transactions on Information Theory*, 2011, **57**(7): 4680−4688

24 Donoho D L, Tsaig Y, Drori I, Starck J L. Sparse solution of underdetermined systems of linear equations by stagewise orthogonal matching pursuit. *IEEE Transactions on Information Theory*, 2012, **58**(2): 1094−1121

25 Marden J R, Arslan G, Shamma J S. Cooperative control and potential games. *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics*, 2009, **39**(6): 1393−1407

26 Li P, Duan H. A potential game approach to multiple UAV cooperative search and surveillance. *Aerospace Science and Technology*, 2017, **68**: 403−415

27 Yang A Y, Sastry S S, Ganesh A, Ma Y. Fast l_1 -minimization algorithms and an application in robust face recognition: A review. In: Proceedings of the 17th IEEE International Conference on Image Processing. Hong Kong, China: IEEE, 2010. 1849−1852

28 Olfati-Saber R. Distributed Kalman filtering for sensor networks. In: Proceedings of the 46th IEEE Conference on Decision and Control. New Orleans, LA, USA: IEEE, 2007. 5492−5498

张岱峰 北京航空航天大学自动化科学与电气工程学院博士研究生. 2013 年于合肥工业大学获得学士学位, 2016 年于北京航空航天大学获得硕士学位. 主要研究方向为多智能体协调控制与决策. E-mail: zdfskh@163.com
(**ZHANG Dai-Feng** Ph. D. candidate at the School of Automation Science and Electrical Engineering, Beihang University. He received his bachelor degree from Hefei University of Technology in 2013, and the master degree from Beihang University in 2016. His main research interest is the cooperative control and decision of multi-agent systems.)

段海滨 北京航空航天大学自动化科学与电气工程学院长聘教授. 2005 年于南京航空航天大学获博士学位, 分别于 2007 年、2011 年在新加坡国立大学、韩国水源大学从事访问学者研究. 主要研究方向为仿生智能, 无人机自主控制. 本文通信作者.
E-mail: hbduan@buaa.edu.cn
(**DUAN Hai-Bin** Long-term professor at the School of Automation Science and Electrical Engineering, Beihang University. He received his Ph. D. degree from Nanjing University of Aeronautics and Astronautics (NUAA) in 2005. He was an academic visitor of National University of Singapore (NUS) in 2007, a senior visiting scholar of the University of Suwon (USW) of South Korea in 2011. His research interest covers bio-inspired intelligence, and autonomous control of unmanned aerial vehicles. Corresponding author of this paper.)