文章编号: 1001-0920(2019)11-2297-06 DOI: 10.13195/j.kzyjc.2019.0046

多传感器系统的最优线性欺骗攻击设计

叶 丹[1,2†], 王吉言[1]

(1. 东北大学 信息科学与工程学院，沈阳 110004；
2. 东北大学 流程工业综合自动化国家重点实验室，沈阳 110004)

摘 要: 从攻击者的角度研究多传感器系统的安全性问题, 该系统配备有分散式卡尔曼滤波器和χ^2检测器. 恶意攻击者通过修改新息序列以达到破坏系统性能的目的. 为了最大程度地破坏系统性能,以数学期望的形式推导出子系统误差协方差表达式,并量化其与融合误差协方差的关系. 此外,结合矩阵理论,分析受攻击前后系统性能指标的变化并给出可躲避χ^2检测器的最优线性欺骗攻击形式. 最后,通过一个数值仿真例子验证所提出攻击策略的有效性.

关键词: 多传感器系统；安全性；线性欺骗攻击；分散式状态估计；χ^2检测器；最优攻击策略

中图分类号: TP273 **文献标志码:** A

Design of optimal linear deception attack for multi-sensor system

YE Dan[1,2†], *WANG Ji-yan*[1]

(1. College of Information Science and Engineering，Northeastern University，Shenyang 110004，China；2. State Key Laboratory of Synthetical Automation of Process Industries，Northeastern University，Shenyang 110004，China)

Abstract: A security issue in multi-sensor systems is investigated from the standpoint of a malicious attacker. The considered system is equipped with a decentralized Kalman filter and χ^2 detectors. A malicious attacker intends to destroy the system performance by modifying the measurement innovation. To damage the system performance as much as possible, we derive the subsystems error covariances in the form of mathematical expectations and then quantify their relation with the error covariance of the fused system. Furthermore, by utilizing the matrix theory, we analyze the difference of performance metrics before and after an attack. And the optimal linear deception attack strategy can be obtained, which can successfully avoid being detected by the χ^2 detector. Finally, a numerical example is given to demonstrate the effectiveness of the proposed attack strategy.

Keywords: multi-sensor system；security；linear deception attack；decentralized state estimation；χ^2 detector；optimal attack strategy

0 引 言

随着感知、计算、通信、控制等技术的不断发展与融合,信息物理系统(cyber-physical systems, CPSs)得到迅猛发展,其包括单元级、系统级、SOS级(system of systems)3种规模的体系架构. 对于生产规模较大、生产要求较高的系统,高精度状态测量值是必须的, 因此,智能化多传感器网络系统应运而生,其广泛应用于航空航天、环境与生态监测、智能电网、智能交通等领域[1-3]. 对于多传感器系统的状态测量,文献[4-6]研究了具有较高鲁棒性的分散式卡尔曼滤波器,并利用权重矩阵得到了系统的最优状态估计值. 由于信息物理系统通过无线网络进行传感器与控制器的交互,导致系统信息易被恶意攻击者获得,从而使系统网络或物理过程遭受潜在威胁并造成严重的破坏[7]. 因此,研究信息物理系统的安全性问题至关重要.

目前,对于CPSs安全性问题的研究主要从攻击者和防御者两个角度进行分析. 从防御者角度出发,研究主要集中在对恶意攻击的检测与识别上[8-9]. 针对传感器和执行器攻击,Lu等[10]设计了一种利用观测器估计值减小攻击危害的安全控制器. 基于数据包接受率的概念,文献[11]提出了一种针对固定时间窗口下拒绝服务(denial of service, DOS)攻击的监控策略. 在此基础上,设计了一种协同补偿机制来保证

收稿日期: 2019-01-08；**修回日期:** 2019-04-19.
基金项目: 国家自然科学基金项目(61773097)；中央高校基本科研专项业务费资金项目(160402004).
责任编委: 左志强.
†通讯作者. E-mail: yedan@ise.neu.edu.cn.

被攻击系统的性能. 在系统部分传感器绝对可靠的假设下,通过分析多传感器网络中各组数据的关系,文献[12]给出一种数据融合与验证算法以提高对线性欺骗攻击的检测精度.

上述研究针对不同攻击策略设计相应的防御机制以维持系统性能,而从恶意攻击者角度,现有文献通常是设计有效的攻击策略以达到破坏系统性能的目的. 典型的攻击策略包括DoS攻击和欺骗攻击两大类. 利用DoS攻击易实现性和高破坏性的特点,文献[13]研究了能量约束条件下的最优攻击调度问题,从而使系统估计误差协方差达到最大. 文献[14]通过构建马尔可夫博弈框架来分析DoS攻击者与CPSs之间的交互决策过程. 针对多传感器系统,文献[15]研究了DoS攻击者能力受限而无法阻断所有信道时最优攻击通道的选择问题. 不同于DoS攻击阻塞通信信道的攻击方式,欺骗攻击通过精心构造虚假数据进而篡改目标系统信息以实现攻击效果. 文献[16-17]在欺骗攻击构造过程中考虑了系统状态分析与异常检测机制,从而使攻击具备一定的隐身性,进而对系统性能造成更加严重的破坏. 基于相对熵理论,文献[18-20]提出ϵ隐身性概念以衡量线性时不变系统中可加入的攻击大小. 考虑系统新息序列,文献[21]设计了一种可以欺骗χ^2检测器的线性攻击策略,并给出了攻击效果最优时的攻击形式. 在此基础上,文献[22]进一步分析了线性攻击策略对含有乘性噪声系统的影响. 为了使系统状态达到攻击者的目标状态值,文献[23]给出了一个设计最优攻击的充分条件. 对于多传感器系统,文献[24]考虑了测量精度矩阵已知且偏序排列时最优的传感器攻击调度问题,并在攻击者能力受限的情况下设计可行的攻击策略对传感器测量数据进行修改.

虽然已有的一些文章涉及多传感器系统的安全问题,但值得注意的是,针对欺骗攻击下系统性能变化的分析相对缺乏. 鉴于此,本文考虑配备有χ^2检测器和分散式卡尔曼滤波器的多传感器系统,并致力于研究该系统中的最优线性欺骗攻击策略. 主要贡献概括如下:

1) 区别于文献[21]研究的单传感器系统,本文从攻击者的角度出发,考虑了多传感器融合系统的最优线性欺骗攻击问题;

2) 从数学期望的角度推导出线性欺骗攻击下多传感器系统的状态估计误差协方差表达式,并给出子系统和融合系统状态误差协方差矩阵之间的定量关系式;

3) 结合多传感器融合系统状态估计性能指标,给出多传感器系统最优线性欺骗攻击的具体形式,并证明该攻击策略的有效性.

说明: $\boldsymbol{R}^n$表示n维欧几里得空间, X'和$\mathrm{tr}X$分别表示矩阵X的转置和矩阵的迹, I_n表示n维单位矩阵, $\mathrm{E}\{\cdot\}$和$\mathrm{Pr}\{\cdot\}$分别表示随机事件的数学期望和概率, δ_{ij}表示克罗·狄利克雷函数, $\mathcal{N}(\mu,\Pi)$表示均值为μ方差为Π的高斯分布, $\mathcal{B}(1,p)$表示参数为p的伯努利分布.

1 问题建立

本文考虑的线性攻击下的CPS如图1所示. 系统中配备有多组智能传感器[21]、χ^2检测器和分散式卡尔曼滤波器. 智能传感器对采集到的数据进行预处理,并通过无线信道将新息序列传输到滤波器. 由于无线通道具有开放、广播、共享的特性,使得攻击者更容易对其进行破坏.

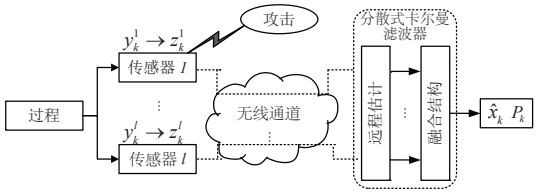

图 1 攻击下的系统框图

1.1 系统描述

图1中的多传感器控制系统描述如下:

$$x_{k+1} = Ax_k + \omega_k, \tag{1}$$

$$y_k^i = C_i x_k + \nu_k^i,\ i = 1,2,\cdots,l. \tag{2}$$

其中: $x_k \in \boldsymbol{R}^n$为系统状态向量, $y_k^i \in \boldsymbol{R}^m$为第$i$组传感器的测量值; $\omega_k \in \boldsymbol{R}^n$和$\nu_k^i \in \boldsymbol{R}^m$分别为系统噪声和测量噪声,其满足均值为零、方差为$\mathrm{E}[\omega_k\omega_t'] = \delta_{kt}Q(Q \geqslant 0)$和$\mathrm{E}[\nu_k^i(\nu_t^j)'] = \delta_{kt}\delta_{ij}R_i(R_i \geqslant 0)$的高斯分布. 系统初始状态为$x_0 \sim \mathcal{N}(0,\Pi_0)$,且$x_0$、$\nu_k$与$\omega_k$分别相互独立[20]. 假设$(A,C_i)$是可检测的,且$(A,\sqrt{Q})$是稳定的.

分散式卡尔曼滤波器由两部分构成: 局部卡尔曼滤波器和融合结构. 前者用于估计系统的状态,后者根据确定的融合算法计算全局最优估计值[4]. 根据第$i(i = 1,2,\cdots,l)$组传感器的测量值,有如下卡尔曼滤波方程:

$$\begin{aligned}
&\hat{x}_{k+1}^{i-} = A\hat{x}_k^i,\\
&P_{k+1}^{i-} = AP_k^iA' + Q,\\
&K_{k+1}^i = P_{k+1}^{i-}C_i'(C_iP_{k+1}^{i-}C_i' + R_i)^{-1},\\
&\hat{x}_{k+1}^i = \hat{x}_{k+1}^{i-} + K_{k+1}^iz_{k+1}^i,\\
&P_{k+1}^i = (I_n - K_{k+1}^iC_i)P_{k+1}^{i-}.
\end{aligned}$$

其中第i组新息序列$z_{k+1}^i \sim \mathcal{N}(0, P_z^i)$满足下式:

$$z_{k+1}^i = y_{k+1}^i - C_i\hat{x}_{k+1}^{i-}.$$

为了得到多传感器控制系统状态的最优估计值,采用分散式卡尔曼滤波器进行状态估计. 定义如下融合权重矩阵:

$$M_1 + M_2 + \cdots + M_l = I_n,$$
$$\hat{x}_k = M_1\hat{x}_k^1 + M_2\hat{x}_k^2 + \cdots + M_l\hat{x}_k^l.$$

根据随机变量的数学期望和两层融合结构,可以得出最优融合权重矩阵满足下式:

$$M = \Sigma^{-1}e(e'\Sigma^{-1}e)^{-1}. \tag{3}$$

其中:$e = [I_n, \cdots, I_n]'$为$nl \times n$维的矩阵,$\Sigma \triangleq (P_{k+1}^{ij})(i = 1, 2, \cdots, l)$为$nl \times nl$维的对称正定矩阵,$P_{k+1}^{ij}(P_{k+1}^i, i = j)$为系统的互协方差矩阵.

多传感器系统的最优状态估计值$\hat{x}$和融合误差协方差$\mathcal{P}$满足下式:

$$\hat{x} = M'[\hat{x}_1', \hat{x}_2', \cdots, \hat{x}_l']',$$
$$\mathcal{P} = \mathrm{E}[\hat{x}\hat{x}'] = M'\Sigma M. \tag{4}$$

1.2 线性欺骗攻击模型

假设1 攻击者有能力截取无线信道中传输的信息并通过线性攻击对新息序列进行修改. 此外,假设攻击者有能力获取系统参数矩阵A, C_i, Q, R_i.

考虑如下线性欺骗攻击:

$$\tilde{z}_{k+1}^i = \alpha_{k+1}[\bar{T}_i z_{k+1}^i + b_{k+1}^i] + z_{k+1}^i. \tag{5}$$

其中:$\bar{T}_{k+1}^i = T_{k+1}^i - I_m, T_{k+1}^i$为任意大小的攻击矩阵;$\alpha_{k+1} \sim \mathcal{B}(1, \varepsilon_{k+1}), b_{k+1}^i \sim \mathcal{N}(0, L)(L > 0)$与$z_{k+1}$相互独立,且假设所有传感器在相同时刻满足同一伯努利分布. 为了使证明过程更为简洁,下文使用T_i表示T_{k+1}^i.

从攻击者的角度考虑,其目的是在系统中注入可欺骗χ^2检测器的攻击,从而破坏系统性能. 系统性能指标[4]表示如下:

$$J = \mathrm{tr}\tilde{\mathcal{P}}_k.$$

注1 多传感器系统中,分散式卡尔曼滤波器用于估计系统状态以获得准确的状态值(4),其估计效果由状态误差协方差矩阵$\mathcal{P}$衡量. 而攻击者旨在破坏系统的状态估计值,因此从误差协方差角度量化攻击效果是合理的.

恶意攻击在χ^2检测器下保持隐匿性的条件为系统受攻击前后的新息序列具有相同的统计特性,即

$$\mathrm{E}[\tilde{z}_{k+1}^i(\tilde{z}_{k+1}^j)'] = \mathrm{E}[z_{k+1}^i(z_{k+1}^j)']. \tag{6}$$

定义$\bar{P}_{ij} = AP_k^{ij}A' + Q$,则

$$\mathrm{E}[z_{k+1}^i(z_{k+1}^j)'] =$$
$$C_i(AP_k^{ij}A' + Q)C_j' + \mathrm{E}[\nu^i(\nu^j)'] =$$
$$C_i\bar{P}_{ij}C_j' + \delta_{ij}R_i \triangleq P_z^{ij}, \tag{7}$$
$$\mathrm{E}[\tilde{z}_{k+1}^i(\tilde{z}_{k+1}^j)'] =$$
$$\mathrm{E}[\{\alpha_{k+1}(\bar{T}_i z_{k+1} + b_{k+1}^i) + z_{k+1}^i\}\times$$
$$\{\alpha_{k+1}(\bar{T}_j z_{k+1}^j + b_{k+1}^j) + z_{k+1}^j\}'] \overset{(a)}{=}$$
$$\varepsilon_{k+1}(\bar{T}_i P_z^{ij}\bar{T}_j' + \bar{T}_i P_z^{ij} + P_z^{ij}\bar{T}_j' + \delta_{ij}L) + P_z^{ij}, \tag{8}$$

其中(a)成立的条件是α满足伯努利分布.

结合式(6)~(8),存在如下隐匿性条件:

$$T_i P_z^{ij} T_j - P_z^{ij} \leqslant 0,\ i, j = 1, 2, \cdots, l. \tag{9}$$

注2 χ^2检测器具有较高的灵敏性、准确性,广泛应用于系统安全分析中[1],其原理是利用残差计算卡方值$g_k^i = (z_k^i)'(P_z^i)^{-1}z_k^i$. 本文中,假设多传感器系统中$l$个检测器独立地监测每个无线信道. 因此,式(9)可表示为$T_i P_z^i T_i - P_z^i \leqslant 0$,意味着融合后误差协方差$\tilde{\mathcal{P}}$的大小受子系统攻击矩阵$T_i(i = 1, 2, \cdots, l)$大小的限制.

2 线性欺骗攻击下的误差协方差分析

本节分析多传感器融合系统的状态误差协方差,并给出融合前后状态误差协方差之间的关系.

当系统中存在线性欺骗攻击时,给出如下状态估计值:

$$\hat{\tilde{x}}_{k+1}^{i-} = A\hat{\tilde{x}}_k^i, \tag{10}$$
$$\hat{\tilde{x}}_{k+1}^i = \hat{\tilde{x}}_{k+1}^{i-} + K_i\tilde{z}_{k+1}^i. \tag{11}$$

引理1 对于任意受线性欺骗攻击威胁的子系统,其后验误差互协方差可表示为

$$\begin{aligned}\tilde{P}_{k+1}^{ij} = {} & A\tilde{P}_k^{ij}A' + Q + K_i(P_z^{ij} + \varepsilon_{k+1}\bar{T}_i P_z^{ij}\bar{T}_j' + \\ & \varepsilon_{k+1}L + \varepsilon_{k+1}\bar{T}_i P_z^{ij} + \varepsilon_{k+1}P_z^{ij}\bar{T}_j')K_j' - \\ & \bar{P}_{ij}C_j'(\varepsilon_{k+1}\bar{T}_j' + I_n)K_j' - \\ & K_i(\varepsilon_{k+1}\bar{T}_i + I_n)C_i\bar{P}_{ij}.\end{aligned} \tag{12}$$

证明 根据系统状态的迭代关系式,线性欺骗攻击的先验和后验估计误差定义为

$$\tilde{e}_{k+1}^{i-} \triangleq x_{k+1} - \hat{\tilde{x}}_{k+1}^{i-}, \tag{13}$$
$$\tilde{e}_{k+1}^i \triangleq x_{k+1} - \hat{\tilde{x}}_{k+1}^i. \tag{14}$$

由上述定义以及(1)和(10),可得$\tilde{e}_{k+1}^{i-} = A\tilde{e}_k^i + \omega_k$.

考虑受攻击下的先验误差协方差

$$\tilde{P}_{k+1}^{ij-} = \mathrm{E}[\tilde{e}_{k+1}^{i-}(\tilde{e}_{k+1}^{j-})'] =$$
$$\mathrm{E}[\{A\tilde{e}_k^i + \omega_k\}\{A\tilde{e}_k^j + \omega_k\}'] \overset{(b)}{=}$$
$$A\tilde{P}_k^{ij}A' + Q. \tag{15}$$

由上述定义和式(15),系统后验误差协方差可表

示为

$$\tilde{P}^{ij}_{k+1}=\mathrm{E}[\tilde{e}^{i}_{k+1}(\tilde{e}^{j}_{k+1})']=$$
$$\mathrm{E}[(\tilde{e}^{i-}_{k+1}-K_i\tilde{z}^{i}_{k+1})(\tilde{e}^{j-}_{k+1}-K_j\tilde{z}^{j}_{k+1})]=$$
$$\tilde{P}^{ij-}_{k+1}-\mathrm{E}[\tilde{e}^{i-}_{k+1}(\tilde{z}^{j}_{k+1})'K'_j]-\mathrm{E}[K_i\tilde{z}^{i}_{k+1}(\tilde{e}^{j-}_{k+1})']+$$
$$\mathrm{E}[K_i\tilde{z}^{i}_{k+1}(\tilde{z}^{j}_{k+1})'K'_j]. \tag{16}$$

结合式(5),式(16)中第2项可表示为

$$\mathrm{E}[\tilde{e}^{i-}_{k+1}(\tilde{z}^{j}_{k+1})'K'_j]=$$
$$\mathrm{E}[\tilde{e}^{i-}_{k+1}\{\alpha(\bar{T}z^{j}_{k+1}+b^{j}_{k+1})'+(z^{j}_{k+1})'\}K'_j]=$$
$$\mathrm{E}[\tilde{e}^{i-}_{k+1}(z^{j}_{k+1})'\bar{T}'_jK'_j\alpha]+\mathrm{E}[\tilde{e}^{i-}_{k+1}(z^{j}_{k+1})'K'_j], \tag{17}$$

其中

$$\mathrm{E}[\tilde{e}^{i-}_{k+1}(z^{j}_{k+1})'\bar{T}'_jK'_j\alpha_{k+1}]=$$
$$\mathrm{E}[\{A\tilde{e}^{i}_{k}+\omega_k\}\{A(x_k-\hat{x}^{j}_{k})+\omega_k\}'C'_j\bar{T}'_jK'_j\alpha_{k+1}]\overset{(c)}{=}$$
$$\varepsilon_{k+1}\mathrm{E}[A\tilde{e}^{i}_{k}(x_k-\hat{x}^{j}_{k})'A'+\omega_k\omega'_k]C'_j\bar{T}'_jK'_j\overset{(d)}{=}$$
$$\varepsilon_{k+1}\mathrm{E}[A(x_k-\hat{x}^{i}_{k})(x_k-\hat{x}^{j}_{k})'A'+\omega_k\omega'_k]C'_j\bar{T}'_jK'_j=$$
$$\varepsilon_{k+1}(AP^{ij}_{k}A'+Q)C'_j\bar{T}'_jK'_j=$$
$$\varepsilon_{k+1}\bar{P}_{ij}C'_j\bar{T}'_jK'_j. \tag{18}$$

类似文献[18]的证明,由正交定理可得$\mathrm{E}[(\hat{\hat{x}}^{i}_{k}-\hat{x}^{i}_{k})(x_k-\hat{x}^{j}_{k})']=0$,因此$\overset{(d)}{=}$成立. 进而可得

$$\mathrm{E}[\tilde{e}^{i-}_{k+1}(\tilde{z}^{j}_{k+1})'K'_j]=$$
$$\varepsilon_{k+1}\bar{P}_{ij}C'_j\bar{T}'_jK'_j+\bar{P}_{ij}C'_jK'_j=$$
$$\bar{P}_{ij}C'_j(\varepsilon_{k+1}\bar{T}'_j+I_n)K'_j. \tag{19}$$

类似的,式(16)第3项可以表示为

$$\mathrm{E}[K_i\tilde{z}^{i}_{k+1}(\tilde{e}^{j-}_{k+1})']=K_i(\varepsilon_{k+1}\bar{T}_i+I_n)C_i\bar{P}_{ij}. \tag{20}$$

将式(8),(15),(19),(20)代入(16)中,可得引理1. □

注3 由式(1),(10),(11)以及卡尔曼滤波器迭代公式可知,x_k与x_0的$k-1$时刻及之前的ω有关,而与ω_k无关. 因此,根据假设x_0和ν_k与ω_k分别相互独立可知,(b)和(c)的推导过程中有$\mathrm{E}[A\tilde{e}^{i}_{k}\omega'_k]=0,\mathrm{E}[\omega_k(x_k-\hat{x}^{j}_{k})'A']=0$成立.

定理1 考虑图1描述的多传感器系统,当线性欺骗攻击(5)在χ^2检测器下保持隐身特性时,融合后的状态误差协方差$\tilde{\mathcal{P}}_{k+1}$与子系统误差协方差$\tilde{P}^{ij}_{k+1}$之间存在如下关系式:

$$\tilde{\mathcal{P}}_{k+1}\leqslant\frac{1}{l^2}\cdot\sum_{i=1}^{l}\sum_{j=1}^{l}\tilde{P}^{ij}_{k+1},\ i,j=1,2,\cdots,l. \tag{21}$$

其中

$$\tilde{P}^{ij}_{k+1}=A\tilde{P}^{ij}_{k}A'+Q+K_iP^{ij}_{z}K'_j-\bar{P}_{ij}C'_j(\varepsilon_{k+1}\bar{T}'_j+$$
$$I_n)K'_j-K_i(\varepsilon_{k+1}\bar{T}_i+I_n)C_i\bar{P}_{ij}, \tag{22}$$
$$P^{ij}_{z}=C_i\bar{P}_{ij}C'_j+\delta_{ij}R_i.$$

证明 定义$\tilde{\Sigma}\triangleq(\tilde{P}^{ij}_{k+1})$. 根据文献[4]提出的方法,存在如下权重矩阵:

$$\tilde{M}=\tilde{\Sigma}^{-1}e(e'\tilde{\Sigma}^{-1}e)^{-1}. \tag{23}$$

受攻击下的误差协方差矩阵表示为

$$\tilde{\mathcal{P}}_{k+1}=\mathrm{E}[x_{k+1}-\hat{\hat{x}}_{k+1}][x_{k+1}-\hat{\hat{x}}_{k+1}]'=\tilde{M}'\tilde{\Sigma}\tilde{M}=$$
$$[\tilde{\Sigma}^{-1}e(e'\tilde{\Sigma}^{-1}e)^{-1}]'\tilde{\Sigma}[\tilde{\Sigma}^{-1}e(e'\tilde{\Sigma}^{-1}e)^{-1}]\overset{(e)}{=}$$
$$\frac{1}{l^2}[(\tilde{\Sigma}^{-\frac{1}{2}}e)'(\tilde{\Sigma}^{\frac{1}{2}}e)]'[(\tilde{\Sigma}^{-\frac{1}{2}}e)'(\tilde{\Sigma}^{-\frac{1}{2}}e)]^{-1}\times$$
$$[(\tilde{\Sigma}^{-\frac{1}{2}}e)'(\tilde{\Sigma}^{\frac{1}{2}}e)]\overset{(f)}{\leqslant}$$
$$\frac{1}{l^2}(\tilde{\Sigma}^{-\frac{1}{2}}e)'(\tilde{\Sigma}^{-\frac{1}{2}}e)=$$
$$\frac{1}{l^2}\sum_{i=1}^{l}\sum_{j=1}^{l}\tilde{P}^{ij}_{k+1},\ i,j=1,2,\cdots,l.$$

由$e'e=lI_n$以及Schwartz矩阵不等式可证(e)和(f)成立.

根据引理1,当攻击(5)满足隐匿性条件(6)时,结合式(7)、(8)、(12)可得(22). □

注4 定理1中误差协方差(22)存在的前提是子系统卡尔曼滤波器是状态稳定的. 由卡尔曼滤波增益矩阵和误差协方差矩阵可从任意初始值收敛到稳定状态的特性可知,上述假设合理[19,21],即存在$\bar{P}_i=\lim\limits_{k\to\infty}P^{i-}_{k},K_i=\bar{P}_iC'_i(C_i\bar{P}_iC_i+R_i)^{-1}$.

3 最优攻击策略

本节将根据定理1,给出最优攻击T_i的形式.

定理2 考虑系统(1)和(2)中的线性欺骗攻击,当攻击者能力受限($\Pr\{\alpha_{k+1}=1\}=\varepsilon$)时,为获得最优的攻击效果,线性欺骗攻击需满足$T_i=-I_n(i=1,2,\cdots,l)$且$b_{k+1}=0$.

证明 从攻击者角度考虑,受攻击时系统性能指标$J(T)$大于无攻击时系统性能指标. 因此,在满足隐匿性条件下,对于任意矩阵Λ有如下不等式存在:

$$\Big[\sum_{i=1}^{l}\sum_{j=1}^{l}\tilde{P}^{ij}_{k+1}\Big]_{H=I+\Lambda}-\Big[\sum_{i=1}^{l}\sum_{j=1}^{l}\tilde{P}^{ij}_{k+1}\Big]_{H=I}\geqslant 0. \tag{24}$$

其中:$H=[H_1,H_2,\cdots,H_l],I=[I_n,\cdots,I_n],\Lambda=[\Lambda_1,\Lambda_2,\cdots,\Lambda_l]$均为$n\times nl$维的矩阵,攻击矩阵$T_i$取值为$H_i$.

对于$\sum\limits_{i=1}^{l}\sum\limits_{j=1}^{l}\tilde{P}^{ij}_{k+1}$中的任一子项$\tilde{P}^{ij}_{k+1}$,当矩阵$\Lambda$和$\tilde{\Lambda}$满足式(9)时,如下条件成立:

$$[\tilde{P}^{ij}_{k+1}]_{\substack{T_i=I_n+\Lambda_i,\\ T_j=I_n+\Lambda_j}}-[\tilde{P}^{ij}_{k+1}]_{T_i,T_j=I_n}\geqslant 0, \tag{25}$$

$$[\tilde{P}^{ij}_{k+1}]_{\substack{T_i=-I_n-\tilde{\Lambda}_i,\\ T_j=-I_n-\tilde{\Lambda}_j}}-[\tilde{P}^{ij}_{k+1}]_{T_i,T_j=-I_n}\leqslant 0. \tag{26}$$

结合式(12), (24), (25)可得

$$\sum_{i=1}^{l}\sum_{j=1}^{l}\varepsilon(\bar{P}^{ij}C_j'\Lambda_j'K_j'+K_i\Lambda_iC_i\bar{P}_{ij})\leqslant 0. \tag{27}$$

根据式(27), 当矩阵$\tilde{\Lambda}$满足式(26)时, 合并所有子项, 可得

$$\Big[\sum_{i=1}^{l}\sum_{j=1}^{l}\tilde{P}_{k+1}^{ij}\Big]_{\tilde{H}=-I-\tilde{\Lambda}}-\Big[\sum_{i=1}^{l}\sum_{j=1}^{l}\tilde{P}_{k+1}^{ij}\Big]_{\tilde{H}=-I}=$$

$$\sum_{i=1}^{l}\sum_{j=1}^{l}\varepsilon(\bar{P}^{ij}C_j'\tilde{\Lambda}_j'K_j'+K_i\tilde{\Lambda}_iC_i\bar{P}_{ij})\leqslant 0. \tag{28}$$

式(28)表示$T=-I$时可得到最大的状态误差协方差. 因此, 多传感器系统中最优线性欺骗攻击形式为$T_i=-I_n, i=1,2,\cdots,l$. □

注5　在多传感器系统(1)和(2)中, 其维数满足$l\geqslant 2$. 当$l=1$时, 上述结果将退化为文献[21]中单系统情况下的结论.

4　数值仿真

本节利用仿真实例表明最优攻击策略的有效性.

例1　考虑如下离散系统方程[25]:

$$x_{k+1}=\begin{bmatrix}0.9035 & 0.0082 & -0.0001\\ 0.0741 & 0.8982 & -0.007\\ 0 & 0 & 0.1327\end{bmatrix}x_k+\begin{bmatrix}0.0955\\ 0.0982\\ 0.0429\end{bmatrix}\omega_k,$$

$$y_k^i=C_ix_k+\nu_k^i.$$

其中: $C_1=I_3, C_2=\begin{bmatrix}1&0&0\\0&1&1\end{bmatrix}$, 过程噪声和测量噪声协方差分别为$Q=I_3, R_1=0.1I_3, R_2=0.1I_2$.

仿真结果如图2和图3所示.

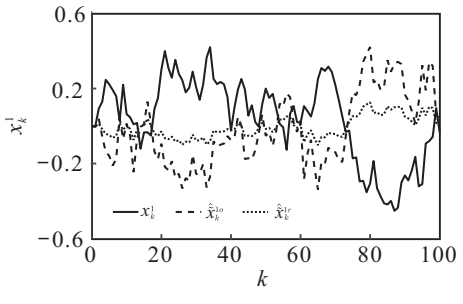

图2　例1系统的状态轨迹

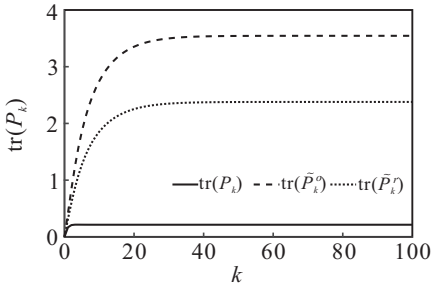

图3　例1系统的性能指标

图2和图3分别表示不同攻击下多传感器融合系统的状态轨迹x_k^1以及性能指标$\mathrm{tr}\tilde{P}$. 其中x_k^1与$\mathrm{tr}(\tilde{P}_k)$、x_k^{1r}与$\mathrm{tr}(\tilde{P}_k^r)$、$x_k^{1o}$与$\mathrm{tr}(\tilde{P}_k^o)$分别表示无攻击、随机攻击以及最优线性欺骗攻击下的情形. 与随机攻击形式比较可知, 最优攻击形式($\tilde{z}_{k+1}=-z_{k+1}$)造成的性能改变量最大, 并且最优攻击下与未受攻击下的系统状态相反. 说明当线性欺骗攻击$T_i=-I(i=1,2,\cdots,l)$时, 攻击效果达到最优.

例2　考虑如下多传感器系统(A,C_i):

$$A=\begin{bmatrix}1&T\\0&1\end{bmatrix},\ C_1=\begin{bmatrix}1&1\\0&1\end{bmatrix},\ C_2=[1\ \ 1].$$

其中: $T=0.25$, 过程噪声与测量噪声协方差为$Q=\mathrm{diag}(0.25T^4,T^2),\ R_1=0.8I,\ R_2=0.6$.

仿真结果如图4和图5所示.

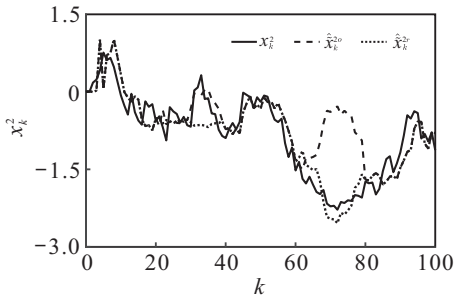

图4　例2系统的状态轨迹

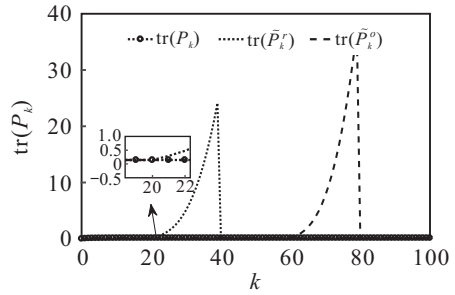

图5　例2系统的性能指标

图4和图5表示不稳定的系统在线性欺骗攻击下状态轨迹和误差协方差的变化. 为便于分析, 图4中仅给出了系统的第2个状态轨迹. 恶意攻击者在[20, 40]和[60, 80]时间段内分别以随机攻击和最优攻击对新息序列进行修改. 可以看出, 在任意大小的攻击下, 不稳定系统的误差协方差矩阵将以指数形式发散到无穷大.

5　结　论

本文研究了多传感器融合系统遭受线性欺骗攻击情况下的安全性问题. 结合矩阵分析理论, 推导出受攻击下系统状态误差协方差的表达, 并给出融合系统与子系统误差协方差之间的定量关系. 此外, 通过对不同攻击形式下系统性能指标变化的分析, 证明了系统中可加入的最优线性欺骗攻击大小为$T_i=$

$-I, i = 1, 2, \cdots, l$. 在未来的研究中,将考虑含有控制输入的系统,并保证线性欺骗攻击下系统的稳定性.

参考文献(References)

[1] Colombo A W, Karnouskos S, Kaynak O, et al. Industrial cyberphysical systems: A backbone of the fourth industrial revolution[J]. IEEE Industrial Electronics Magazine, 2017, 11(1): 6-16.

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

[3] Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.

[4] Sun S L, Deng Z L. Multi-sensor optimal information fusion Kalman filter[J]. Automatica, 2004, 40(6): 1017-1023.

[5] Sun S L, Lin H L, Ma J, et al. Multi-sensor distributed fusion estimation with applications in networked systems: A review paper[J]. Information Fusion, 2017, 38: 122-134.

[6] Tian T, Sun S L, Lin H L. Distributed fusion filter for multi-sensor systems with finite-step correlated noises[J]. Information Fusion, 2019, 46: 128-140.

[7] Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries[J]. Automatica, 2015, 51: 135-148.

[8] Li H Y, Chen Z R, Wu L G, et al. Event-triggered fault detection of nonlinear networked systems[J]. IEEE Transactions on Cybernetics, 2017, 47(4): 1041-1052.

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

[10] Lu A Y, Yang G H. Event-triggered secure observer-based control for cyber-physical systems under adversarial attacks[J]. Information Sciences, 2017, 420: 96-109.

[11] Su L, Ye D. A cooperative detection and compensation mechanism against denial-of-service attack for cyber-physical systems[J]. Information Sciences, 2018, 444: 122-134.

[12] Li Y Z, Shi L, Chen T W. Detection against linear deception attacks on multi-sensor remote state estimation[J]. IEEE Transactions on Control of Network Systems, 2018, 5(3): 846-856.

[13] Zhang H, Cheng P, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint[J]. IEEE Transactions on Automatic Control, 2015, 60(11): 3023-3028.

[14] Li Y Z, Quevedo D E, Dey S, et al. SINR-based dos attack on remote state estimation: A game-theoretic approach[J]. IEEE Transactions on Control of Network Systems, 2017, 4(3): 632-642.

[15] Yang C, Ren X Q, Yang W, et al. Jamming attack in centralized state estimation[C]. Proceedings of the 34th Chinese Control Conference (CCC). Las Vegas: IEEE, 2015: 6530-6535.

[16] Wu G Y, Sun J, Chen J. Optimal data injection attacks in cyber-physical systems[J]. IEEE Transactions on Cybernetics, 2018, 48(12): 3302-3312.

[17] Huang X, Dong J X. Adaptive optimisation-offline cyber attack on remote state estimator[J]. International Journal of Systems Science, 2017, 48(14): 3060-3071.

[18] Bai C Z, Gupta V, Pasqualetti F. On Kalman filtering with compromised sensors: Attack stealthiness and performance bounds[J]. IEEE Transactions on Automatic Control, 2017, 62(12): 6641-6648.

[19] Bai C Z, Pasqualetti F, Gupta V. Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs[J]. Automatica, 2017, 82: 251-260.

[20] Kung E, Dey S, Shi L. The performance and limitations of ϵ-stealthy attacks on higher order systems[J]. IEEE Transactions on Automatic Control, 2017, 62(2): 941-947.

[21] Guo Z Y, Shi D W, Johansson K H, et al. Optimal linear cyber-attack on remote state estimation[J]. IEEE Transactions on Control of Network Systems, 2017, 4(1): 4-13.

[22] Li F F, Yang C, Tang Y. Optimal linear attack on cyber physical systems with multiplicative noise[J]. IEEE Access, 2018, 6: 33318-33328.

[23] Chen Y, Kar S, Moura J M F. Cyber-physical attacks with control objectives[J]. IEEE Transactions on Automatic Control, 2018, 63(5): 1418-1425.

[24] Li F F, Tang Y. False data injection attack for cyber-physical systems with resource constraint[J]. IEEE Transactions on Cybernetics, 2018: 1-10.

[25] Stevens B L, Lewis F L. Aircraft control and simulation[M]. Wiley-Interscience, 2003.

作者简介

叶丹 (1979−), 女, 教授, 博士生导师, 从事信息物理系统安全理论与技术、容错控制、鲁棒控制等研究, E-mail: yedan@ise.neu.edu.cn;

王吉言 (1993−), 男, 硕士生, 从事信息物理系统安全理论与技术的研究, E-mail: JYWang931@163.com.

(责任编辑：孙艺红)