Pure Mathematics 理论数学, 2024, 14(5), 560-566
Published Online May 2024 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2024.145209

Hans汉斯

非线性系统下的虚假信息注入攻击研究

杨修远

上海理工大学理学院，上海

收稿日期：2024年4月19日；录用日期：2024年5月21日；发布日期：2024年5月31日

摘　要

本文提出了一种基于扩展卡尔曼滤波算法的线性攻击策略。在单传感器网络的非线性系统框架下，通过向数据传输过程中被截获的新息序列注入虚假数据，从而达到攻击该网络系统、使其性能下降的目的。这样不仅有效降低了系统的稳定性，并且能高效地规避被虚假数据检测器发现的风险。最后利用扩展卡尔曼滤波推导出攻击过程中远端估计器的误差协方差矩阵，并且通过误差协方差矩阵的演化合理地展现出系统性能的退化。

关键词

扩展卡尔曼滤波，线性攻击策略，虚假数据

Research on Disinformation Injection Attacks in Nonlinear Systems

Xiuyuan Yang

College of Science, University of Shanghai for Science and Technology, Shanghai

Received: Apr. 19th, 2024; accepted: May 21st, 2024; published: May 31st, 2024

Abstract

In this paper, we present a linear attack strategy based on the Extended Kalman Filter (EKF) algorithm. Within the framework of a single sensor network with nonlinear systems, the objective is to attack the network system and degrade its performance by injecting false data into the intercepted new information sequences during the data transmission process. This not only effectively reduces the stability of the system but also efficiently avoids the risks detected by false data detectors. Finally, utilizing the Extended Kalman Filter, the error covariance matrix of the remote estimator during the attack process is derived, demonstrating the degradation of system performance reasonably through the evolution of the error covariance matrix.

文章引用: 杨修远. 非线性系统下的虚假信息注入攻击研究[J]. 理论数学, 2024, 14(5): 560-566.
DOI: 10.12677/pm.2024.145209

Keywords

Extended Kalman Filter, Linear Attack Strategy, False Data

1. 引言

进入二十一世纪以来，信息产业飞速发展，科技的突破不断影响着人们日常生活。但与此同时，原有的物理系统已经无法适应人们对新一代生产装备网络化、信息化和智能化的需求。因此，信息物理系统应运而出[1] [2]。

然而，信息物理系统作为一种开放是的网络智能信息系统，在量测和控制数据的方式是通过网络空间进行集成于交互，这具有一定的脆弱性，带来了新的安全威胁风险。正如[3]中所示，经过调查发现了多种针对信息物理系统的网络攻击形式，大致可以分为如下几类：虚假数据注入[4]，拒绝服务式[5]，窃听攻击和零动态攻击等。

目前，针对信息物理系统安全控制问题的研究可以从防御和攻击两个角度展开。从防御者角度来看，研究的主要目的在于如何有效识别与检测恶意攻击[6] [7]；而从攻击者角度来看，研究的目的在于绕过系统检测成功攻击网络，从而影响其性能。

站在攻击者角度来看，现有文献主要思路为：通过破坏性极强的攻击手段来打破系统稳定，如 FDI 攻击和 DoS 攻击。在[8]中，作者利用上述攻击方式构建出最优攻击策略，是系统存在能量约束时期望平均估计误差最大；而在[9]中，作者使用独立组件分析系统架构以及异常数据检测器存在的天然缺陷，从而使得攻击具有一定隐蔽性来达到攻击系统的目的；在[10]中，作者通过修改系统的新息序列设计了一种可以逃避传统检测气的最优线性欺骗攻击策略。

上述内容主要介绍了国内外专家关于信息物理系统在线性环境下的攻击与检测研究，然而对于非线性系统在该方面的研究也是不能忽视的。周雪[11]等人通过在网络数据传输过程中注入虚假信息，利用事件触发机制对扩展卡尔曼滤波参数进行优化，从而保障了网络系统的稳定性；在文献[12]中，作者利用极端梯度提升算法进行追踪预测，利用无迹卡尔曼滤波处理后的预测值有效的降低了 FDI 攻击对网络系统的影响；在文献[13]中，由于受到 DoS 攻击的影响，作者通过优化传统的无迹卡尔曼滤波滤波算法实现了对电网状态的准确估计。

因此，本文在上述研究背景和框架下，提出了一种基于扩展卡尔曼滤波，在非线性信息物理系统的数据传输过程中，通过向截获的新息序列注入线性欺骗数据的方式，来干扰系统网络性能的算法，并通过定理证明阐述了远端估计器的误差协方差矩阵的演化，从而刻画出在该攻击策略下网络系统性能的衰退。

因为本文是在非线性系统的基础上使用扩展卡尔曼滤波算法来进行虚假信息注入的攻击策略研究，因此本文假定读者具备扩展卡尔曼滤波算法的相关知识储备。

2. 问题定式化

本节考虑一个如下的带有高斯白噪声的离散非线性系统：

$$\begin{cases} x_{t+1} = f\left(x_t\right) + \omega_t \\ y_t = h\left(x_t\right) + \upsilon_t \end{cases} \tag{1}$$

其中 $\omega_t \in \mathbb{R}^l$ 和 $\upsilon_t \in \mathbb{R}^m$ 分别为系统的过程噪声和测量噪声，二者为互不相关的高斯白噪声，均值均为 0，协方差分别为 Q_t 和 R_t。上述状态方程中的 $f\left(\cdot\right)$ 和观测方程中的 $h\left(\cdot\right)$ 均为非线性函数，根据第二节中有关卡尔曼滤波的介绍，利用泰勒公式对上述非线性系统进行展开并且舍去二阶导数及以上项可得：

$$f\left(x_t\right) \approx f\left(\hat{x}_t\right) + F_t\left(x_t - \hat{x}_t\right) \tag{2}$$

其中，$F_t = \left.\dfrac{\mathrm{d}f}{\mathrm{d}x_t}\right|_{x_t=\hat{x}_t}$ 为 $f\left(\cdot\right)$ 对 x_t 求导所得的雅可比矩阵，具体表达式如下：

$$F_t = J_f = \begin{bmatrix} \dfrac{\partial f_1}{\partial x_1} & \cdots & \dfrac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial f_n}{\partial x_1} & \cdots & \dfrac{\partial f_n}{\partial x_n} \end{bmatrix}$$

$$h\left(x_t\right) \approx h\left(\hat{x}_t^-\right) + H_t\left(x_t - \hat{x}_t^-\right) \tag{3}$$

其中，$\hat{x}_k^- = f\left(\hat{x}_{t-1}\right)$，$H_t = \left.\dfrac{\mathrm{d}h}{\mathrm{d}x_t}\right|_{x_t=\hat{x}_t^-}$ 为 $h\left(\cdot\right)$ 对 x_t 求导所得的雅可比矩阵，具体表达式如下：

$$H_t = J_h = \begin{bmatrix} \dfrac{\partial h_1}{\partial x_1} & \cdots & \dfrac{\partial h_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \dfrac{\partial h_m}{\partial x_1} & \cdots & \dfrac{\partial h_m}{\partial x_n} \end{bmatrix}$$

根据上述的介绍和扩展卡尔曼滤波相关知识，我们定义观测值 y_t 和预测值 $\hat{x}_k^-$ 的偏差为 z_t，称之为新息序列，其中 $z_t = y_t - H_t\hat{x}_t^-$。显然可以得到关于 z_t 的如下性质：

$$\begin{cases} E\left[z_t z_t^{\mathrm{T}}\right] = H_t P_t H_t^{\mathrm{T}} + R_t \triangleq \overline{P} \\ E\left[z_t\right] = E\left[y_t\right] - E\left[H_t\hat{x}_t^-\right] = 0 \end{cases} \tag{4}$$

其中 P_t 为系统的误差协方差矩阵。公式(4)说明新息序列 z_t 均值为 0，协方差为 $\overline{P} \triangleq H_t P_t H_t^{\mathrm{T}} + R_t$。

3. 线性攻击策略下远端误差协方差矩阵的演化

通过恶意攻击形式注入新的新息序列 z_t 来修改系统数据，我们提出一种线性攻击策略，在 k 时刻，此攻击策略表达形式如下：

$$\tilde{z}_t = \Gamma_t z_t + m_t \tag{5}$$

其中，$\Gamma_t \in \mathbb{R}^{m\times m}$ 是一个攻击矩阵，包含所有的线性攻击形式，$m_t \sim N\left(0, L\right)$，$L > 0$ 是一个和 z_t 独立同分布的高斯随机变量。$\tilde{z}_t$ 表示被攻击后受到修改的新息序列，此时即可被视为虚假数据，并且 $\tilde{z}_t \sim N\left(0, \Gamma_t\overline{P}\Gamma_t^{\mathrm{T}} + L\right)$。

图 1 即上述线性攻击策略的施展流程图。当开关为 S1 时，此时系统正常运行，远端估计器能够准确接收到数据包，与此同时，入侵者也能够记录传输过来的数据；当开关为 S2 时，此时入侵者通过无线信道开始施加线性攻击策略，对系统网络发起攻击。

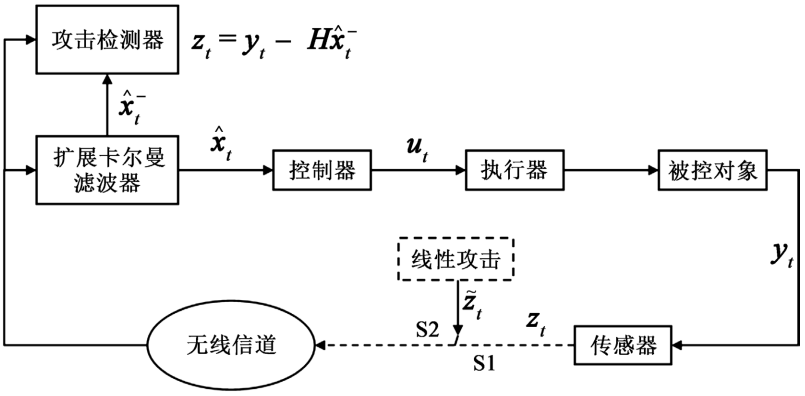

Figure 1. Linear attack strategy flowchart
图 1. 线性攻击策略流程图

入侵者的目的是为了扰乱系统状态，同时保证注入的虚假信息不会被数据检测器发现，所以为了保证让上述提出的攻击策略顺利通过检测器的检查就成了当前的主要任务。根据相关检测标准可知，如果修改后注入到系统中的新息序列 $\tilde{z}_t$ 满足高斯分布 $N\left(0,\bar{P}\right)$ 即可。因此可得：

$$\Gamma_t \bar{P} \Gamma_t^{\mathrm{T}} + L = \bar{P} \tag{6}$$

变形可得：

$$\bar{P} - \Gamma_t \bar{P} \Gamma_t^{\mathrm{T}} = L \geq 0 \tag{7}$$

因此，对于拥有系统完整系统的黑客，可以根据截获的系统信息准确计算出估计误差协方差，先选择满足 $\bar{P} - \Gamma_t \bar{P} \Gamma_t^{\mathrm{T}} \geq 0$ 的攻击矩阵，接着再根据 $L = \bar{P} - \Gamma_t \bar{P} \Gamma_t^{\mathrm{T}} \geq 0$ 选择随机变量 m_t，这样就可以得到满足条件的线性攻击策略。

系统在上述的线性攻击策略 $\tilde{z}_t = \Gamma_t z_t + m_t$ 的影响下，我们给出如下远程估计器的状态估计：

$$\hat{\hat{x}}_t^- = f\left(\hat{\hat{x}}_{t-1}\right) \tag{8}$$

$$\hat{\hat{x}}_t = \hat{\hat{x}}_t^- + K_t \tilde{z}_t \tag{9}$$

其中，K_t 是非线性系统下对应的扩展卡尔曼增益。如果上述攻击策略满足公式(7)，那么检测器就无法检测出虚假数据的存在，从而导致远端估计器产生的状态估计 $\hat{\hat{x}}_k$ 偏离系统的实际状态，接下来定理 1 就展示了在这种线性攻击策略下估计误差协方差的演化。

定理 1 一个非线性系统被上述线性攻击策略攻击时，其在远端估计处的估计误差协方差具有如下形式：

$$\begin{aligned} \tilde{P}_{t+1} = {} & F_t \tilde{P}_t F_t^{\mathrm{T}} + Q_t - \kappa_t H_{t+1}^{\mathrm{T}} \Gamma_{t+1}^{\mathrm{T}} K_{t+1}^{\mathrm{T}} - K_{t+1} \Gamma_{t+1} H_{t+1} \kappa_t \\ & + K_{t+1} \left[\Gamma_{t+1} \left(H_{t+1} \kappa_t H_{t+1}^{\mathrm{T}} + R_{t+1} \right) \Gamma_{t+1}^{\mathrm{T}} + L \right] K_{t+1}^{\mathrm{T}} \end{aligned} \tag{10}$$

其中 $\kappa \triangleq F_t P_t F_t^{\mathrm{T}} + Q_t$。

证明 根据公式(1)、(8)、(9)和扩展卡尔曼滤波相关知识可以定义受线性欺骗攻击影响下的先验、后验估计误差如下所示：

$$\tilde{e}_{t+1}^- \triangleq x_{t+1} - \hat{\hat{x}}_{t+1}^- \tag{11}$$

$$\tilde{e}_{t+1} \triangleq x_{t+1} - \hat{\hat{x}}_{t+1} \tag{12}$$

因为 $\hat{\hat{x}}_{t+1}^- = f\left(\hat{\hat{x}}_t\right)$ 和 $x_{t+1} = f\left(\hat{\hat{x}}_t\right) + F_t\left(x_t - \hat{\hat{x}}_t\right) + \omega_t$，所以先验误差又可以表示为：

$$\tilde{e}_{t+1}^- = F_t\left(x_t - \hat{\hat{x}}_t\right) + \omega_t = F_t \tilde{e}_t + \omega_t \tag{13}$$

进一步可得，在线性攻击策略影响下，远端估计器的误差协方差为：

$$\tilde{P}_{t+1}^{-}=E\left[\tilde{e}_{t+1}^{-}\left(\tilde{e}_{t+1}^{-}\right)^{\mathrm{T}}\right]=E\left[\left(F_t\tilde{e}_t+\omega_t\right)\left(F_t\tilde{e}_t+\omega_t\right)^{\mathrm{T}}\right]=F_t\tilde{P}_tF_t^{\mathrm{T}}+Q_t \tag{14}$$

其中，为了和之前符号统一，称 $\tilde{P}_{t+1}^{-}$ 为远端估计器的先验误差协方差。根据公式(9)、(11)和(12)可得：

$$\begin{cases}\tilde{e}_{t+1}-\tilde{e}_{t+1}^{-}=\hat{\tilde{x}}_{t+1}^{-}-\hat{\tilde{x}}_{t+1}\\ \tilde{e}_{t+1}=\tilde{e}_{t+1}^{-}-K_{t+1}\tilde{z}_{t+1}\end{cases} \tag{15}$$

进一步可得：

$$\begin{aligned}\tilde{P}_{t+1}&=E\left[\tilde{e}_{t+1}\left(\tilde{e}_{t+1}\right)^{\mathrm{T}}\right]\\&=E\left[\left(\tilde{e}_{t+1}^{-}-K_{t+1}\tilde{z}_{t+1}\right)\left(\tilde{e}_{t+1}^{-}-K_{t+1}\tilde{z}_{t+1}\right)^{\mathrm{T}}\right]\\&=\tilde{P}_{t+1}^{-}-E\left(\tilde{e}_{t+1}^{-}\tilde{z}_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)-E\left[K_{t+1}\tilde{z}_{t+1}\left(\tilde{e}_{t+1}^{-}\right)^{\mathrm{T}}\right]+E\left(K_{t+1}\tilde{z}_{t+1}\tilde{z}_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)\end{aligned} \tag{16}$$

公式(16)中后三项均为未知项，下面分别进行求解。

$$\begin{aligned}E\left(\tilde{e}_{t+1}^{-}\tilde{z}_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)&=E\left[\tilde{e}_{t+1}^{-}\left(\Gamma_{t+1}z_{t+1}+m_{t+1}\right)^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right]\\&=E\left[\tilde{e}_{t+1}^{-}\left(z_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}+m_{t+1}^{\mathrm{T}}\right)K_{t+1}^{\mathrm{T}}\right]\\&=E\left(\tilde{e}_{t+1}^{-}z_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)+E\left(\tilde{e}_{t+1}^{-}m_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)\end{aligned} \tag{17}$$

因为 m_t 是一个独立的高斯随机变量，所以 $E\left(\tilde{e}_{t+1}^{-}m_{t+1}^{\mathrm{T}}\right)=0$。又因为 x_t 仅与 t 时刻之前的 ω 有关，与 t 时刻的 ω 无关，所以易得 $E\left(\tilde{e}_t\omega_t^{\mathrm{T}}\right)=E\left(\omega_t\tilde{e}_t^{\mathrm{T}}\right)=0$。因此式(17)可化简为：

$$\begin{aligned}E\left(\tilde{e}_{t+1}^{-}\tilde{z}_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)&=E\left(\tilde{e}_{t+1}^{-}z_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right)\\&=E\left[\left(F_t\tilde{e}_t+\omega_t\right)\left(y_{t+1}-H_{t+1}\hat{x}_{t+1}^{-}\right)^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right]\\&=E\left\{\left(F_t\tilde{e}_t+\omega\right)\left[F_t\left(x_t-\hat{x}_t\right)+\omega_t\right]^{\mathrm{T}}H_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right\}\\&=E\left[F_t\tilde{e}_t\left(x_t-\hat{x}_t\right)^{\mathrm{T}}F_t^{\mathrm{T}}+\omega_t\omega_t^{\mathrm{T}}\right]H_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\\&=E\left[F_t\left(x_t-\hat{x}_t\right)\left(x_t-\hat{x}_t\right)^{\mathrm{T}}F_t^{\mathrm{T}}+\omega_t\omega_t^{\mathrm{T}}\right]H_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\\&=\left(F_tP_tF_t^{\mathrm{T}}+Q_t\right)H_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\\&=\kappa H_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\end{aligned} \tag{18}$$

接下来处理公式(16)的第三项 $E\left[K_{t+1}\tilde{z}_{t+1}\left(\tilde{e}_{t+1}^{-}\right)^{\mathrm{T}}\right]$，化简可得：

$$\begin{aligned}E\left[K_{t+1}\tilde{z}_{t+1}\left(\tilde{e}_{t+1}^{-}\right)^{\mathrm{T}}\right]&=E\left[K_{t+1}\tilde{z}_{t+1}\left(F_t\tilde{e}_t+\omega_t\right)^{\mathrm{T}}\right]\\&=E\left[K_{t+1}\left(\Gamma_{t+1}z_{t+1}+m_{t+1}\right)\left(F_t\tilde{e}_t+\omega_t\right)^{\mathrm{T}}\right]\\&=E\left[K_{t+1}\Gamma_{t+1}z_{t+1}\left(F_t\tilde{e}_t+\omega_t\right)^{\mathrm{T}}\right]\\&=E\left\{K_{t+1}\Gamma_{t+1}H_{t+1}\left[F_t\left(x_t-\hat{x}_t\right)+\omega_t\right]\left(F_t\tilde{e}_t+\omega_t\right)^{\mathrm{T}}\right\}\\&=K_{t+1}\Gamma_{t+1}H_{t+1}\left(F_tP_tF_t^{\mathrm{T}}+Q_t\right)\\&=K_{t+1}\Gamma_{t+1}H_{t+1}\kappa\end{aligned} \tag{19}$$

最后对公式(16)的尾项化简可得：

$$\begin{aligned} E\left(K_{t+1}\tilde{z}_{t+1}\tilde{z}_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right) &= K_{t+1}E\left[\left(\Gamma_{t+1}z_{t+1}+m_{t+1}\right)\left(\Gamma_{t+1}z_{t+1}+m_{t+1}\right)^{\mathrm{T}}\right]K_{t+1}^{\mathrm{T}} \\ &= K_{t+1}E\left(\Gamma_{t+1}z_{t+1}z_{t+1}^{\mathrm{T}}\Gamma_{t+1}^{\mathrm{T}}\right)K_{t+1}^{\mathrm{T}}+K_{t+1}E\left(m_{t+1}m_{t+1}^{\mathrm{T}}\right)K_{t+1}^{\mathrm{T}} \\ &= K_{t+1}\Gamma_{t+1}E\left(z_{t+1}z_{t+1}^{\mathrm{T}}\right)\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}+K_{t+1}LK_{t+1}^{\mathrm{T}} \end{aligned} \tag{20}$$

其中，对公式(20)中 $E\left(z_{t+1}z_{t+1}^{\mathrm{T}}\right)$ 进一步求解可得：

$$\begin{aligned} E\left(z_{t+1}z_{t+1}^{\mathrm{T}}\right) &= E\left[\left(y_{t+1}-H_{t+1}\hat{x}_{t+1}^{-}\right)\left(y_{t+1}-H_{t+1}\hat{x}_{t+1}^{-}\right)^{\mathrm{T}}\right] \\ &= E\left\{\left\{H_{t+1}\left[F_t\left(x_t-\hat{x}_t\right)+\omega_t\right]+\upsilon_{t+1}\right\}\left\{H_{t+1}\left[F_t\left(x_t-\hat{x}_t\right)+\omega_t\right]+\upsilon_{t+1}\right\}^{\mathrm{T}}\right\} \\ &= H_{t+1}E\left\{\left[F_t\left(x_t-\hat{x}_t\right)+\omega_t\right]\left[F_t\left(x_t-\hat{x}_t\right)+\omega_t\right]^{\mathrm{T}}\right\}H_{t+1}^{\mathrm{T}}+E\left(\upsilon_{t+1}\upsilon_{t+1}^{\mathrm{T}}\right) \\ &= H_{t+1}\left(F_tP_tF_t^{\mathrm{T}}+Q_t\right)H_{t+1}^{\mathrm{T}}+R_{t+1} \\ &= H_{t+1}\kappa H_{t+1}^{\mathrm{T}}+R_{t+1} \end{aligned} \tag{21}$$

代入(20)可得：

$$\begin{aligned} E\left(K_{t+1}\tilde{z}_{t+1}\tilde{z}_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}\right) &= K_{t+1}\Gamma_{t+1}\left(H_{t+1}\kappa H_{t+1}^{\mathrm{T}}+R_{t+1}\right)\Gamma_{t+1}^{\mathrm{T}}K_{t+1}^{\mathrm{T}}+K_{t+1}LK_{t+1}^{\mathrm{T}} \\ &= K_{t+1}\left[\Gamma_{t+1}\left(H_{t+1}\kappa H_{t+1}^{\mathrm{T}}+R_{t+1}\right)\Gamma_{t+1}^{\mathrm{T}}+L\right]K_{t+1}^{\mathrm{T}} \end{aligned} \tag{22}$$

综上，联立式(18)、(19)、(22)，代入式(16)，即可得式(10)成立，故定理 1 成立。

4. 数值模拟

本次数值模拟采用如下所示的非线性模型：

$$\begin{cases} X(t)=f(t)+5\cos(t-1)+\omega(t-1), \\ Z(t)=h(t)+\upsilon(t), \end{cases}$$

其中 $f(t)=0.2\hat{x}_{t-1}+3\hat{x}_{t-1}\Big/\left[1+\left(\hat{x}_{t-1}\right)^2\right]$ 是状态函数；$h(t)=\left(\hat{x}_t^{-}\right)^2\Big/18$ 是观测函数。系统运行的时间为 120 s，在该系统中的 F 和 H 分别为：

$$F(t-1)=\frac{\partial f}{\partial\hat{x}_{t-1}}=0.2+\frac{3\left[1-\left(\hat{x}_{t-1}\right)^2\right]}{\left[1+\left(\hat{x}_{t-1}\right)^2\right]^2},$$

$$H(t)=\frac{\partial h}{\partial\hat{x}_t^{-}}=\frac{\hat{x}_t^{-}}{9},$$

系统运行过程中的过程噪声 ω 和测量噪声 υ，其中 $\omega_t\sim N(0,10)\left(Q_t=10\right)$，$\upsilon_t\sim N(0,1)\left(R_t=1\right)$。在 $(20,40]$ 的时间段对系统进行入侵，通过在 20~40 s 之间入侵者篡改原始数据，并向系统中注入虚假数据。从图 2 中可以看出，上述举动导致轨迹 $\hat{\hat{x}}_t$ 偏离实际值，从而使遭受到线性攻击后的系统状态误差协方差矩阵 P 明显增大，破坏了系统的稳定，使得系统性能退化，因此说明公式(5)提出的攻击策略是有效的。

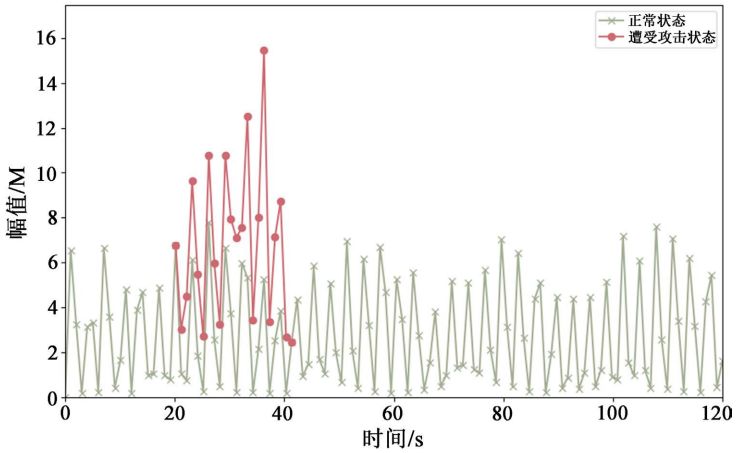

Figure 2. State estimation error
图 2. 状态估计误差

5. 总结

在这项工作中，我们提出了一种基于扩展卡尔曼滤波，在非线性信息物理系统的数据传输过程中，通过向截获的新息序列注入线性欺骗数据的方式，来干扰系统网络性能的算法，并通过定理证明阐述了远端估计器的误差协方差矩阵的演化，从而刻画出在该攻击策略下网络系统性能的衰退。在今后的研究中，我们将从防御方出发，考虑非线性系统下检测虚假信息、维持系统状态稳定的算法，这在实际问题中也具有重要意义。

参考文献

[1] 管晓宏, 关新平, 郭戈. 信息物理融合系统理论与应用专刊序言[J]. 自动化学报, 2019, 45(1): 1-4.

[2] Liu, Y., Peng, Y., Wang, B.L., *et al*. (2017) Review on Cyber-Physical Systems. *IEEE/CAA Journal of Automatica Sinica*, **4**, 27-40. https://doi.org/10.1109/JAS.2017.7510349

[3] Kung, E., Dey, S. and Ling, S. (2017) The Performance and Limitations of ϵ-Stealthy Attacks on Higher Order Systems. *IEEE Transactions on Automatic Control*, **62**, 941-947. https://doi.org/10.1109/TAC.2016.2565379

[4] 陈郁林, 齐冬莲, 李真鸣, 等. 虚假数据注入攻击下的微电网分布式协同控制[J]. 电力系统自动化, 2021, 45(5): 97-103.

[5] 薛田良, 刘希懋, 张赟宁, 等. 周期性拒绝服务攻击下的弹性负荷频率控制[J]. 控制工程, 2021, 28(4): 620-627.

[6] 刘烃, 田决, 王稼舟, 等. 信息物理融合系统综合安全威胁与防御研究[J]. 自动化学报, 2019, 45(1): 5-24.

[7] Li, H., Chen, Z., Wu, L., *et al*. (2017) Event-Triggered Fault Detection of Nonlinear Networked Systems. *IEEE Transactions on Cybernetics*, **47**, 1041-1052. https://doi.org/10.1109/TCYB.2016.2536750

[8] Chen, J., Shi, L., Cheng, P., *et al*. (2015) Optimal Denial-of-Service Attack Scheduling with Energy Constraint. *IEEE Transactions on Automatic Control*, **60**, 3023-3028. https://doi.org/10.1109/TAC.2015.2409905

[9] Wang, X., Mou, W. and Zhu, H. (2021) Effect of Laser Parameters on Optical Stealth Transmission System Performance. *Sensors*, **21**, 5358. https://doi.org/10.3390/s21165358

[10] 叶丹, 王吉言. 多传感器系统的最优线性欺骗攻击设计[J]. 控制与决策, 2019, 34(11): 2297-2302.

[11] 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[J]. 自动化学报, 2020, 46(1): 38-46.

[12] Huang, Y.F., Werner, S., Huang, J., *et al*. (2012) State Estimation in Electric Power Grids: Meeting New Challenges Presented by the Requirements of the Future Grid. *IEEE Signal Processing Magazine*, **29**, 33-43. https://doi.org/10.1109/MSP.2012.2187037

[13] 李雪, 李雯婷, 杜大军, 等. 拒绝服务攻击下基于 UKF 的智能电网动态状态估计研究[J]. 自动化学报, 2019, 45(1): 120-131.