一类混合噪声系统的重放攻击检测方法

符 莎，李 平†，赵民新

(辽宁科技大学 电子与信息工程学院，辽宁 鞍山 114000)

摘 要: 工业现场普遍存在复杂的噪声环境, 其中非高斯噪声和未知有界噪声的混合干扰严重制约了传统重放攻击检测技术的性能. 鉴于此, 提出一种基于状态估计的动态阈值检测算法. 首先, 根据线性系统中未知有界噪声的幅值约束和非高斯噪声的高阶统计属性, 开发依托椭球理论和无偏有限脉冲响应滤波的新型状态估计机制, 以解决现有算法在双重噪声环境下, 因先验统计模型失配而引发的估计性能劣化问题; 然后, 利用系统实时数据设计动态阈值检测策略, 克服重放攻击中固定阈值检测器灵敏度不足的缺陷; 最后, 运用系统残差来构建攻击检测函数, 对系统中潜在的重放攻击进行识别. 仿真结果表明, 所提出方案为此类噪声系统的重放攻击检测提供了一种更加可靠的技术手段, 并展现出优异的适应性.

关键词: 非高斯噪声；未知有界噪声；椭球理论；无偏有限脉冲响应滤波；重放攻击；动态阈值

中图分类号: TP273 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2025.0002

引用格式: 符莎, 李平, 赵民新. 一类混合噪声系统的重放攻击检测方法 [J]. 控制与决策, 2025, 40(10): 3065-3072.

Replay attack detection method for a class of mixed noise systems

FU Sha，*LI Ping*†，*ZHAO Min-xin*

(School of Electronic and Information Engineering， University of Science and Technology Liaoning， Anshan 114000，China)

Abstract: Industrial sites are typically subject to complex noise environments, where mixed interference from non-Gaussian noise and unknown but bounded noise severely degrades the performance of conventional replay attack detection techniques. To address this challenge, a dynamic threshold detection algorithm based on state estimation is proposed. A novel state estimation is developed, leveraging ellipsoid theory and unbiased finite impulse response filtering, which accounts for both the amplitude constraint of unknown but bounded and the higher-order statistical properties of non-Gaussian noise in linear systems. It solves the problem of estimation performance degradation caused by prior statistical model mismatch in the dual noise environment. By employing real-time system information, the dynamic threshold detection strategy is designed to overcome the defect of insufficient sensitivity of the fixed threshold detector in the context of replay attacks. Utilizing the system's residuals, a detection function is formulated to recognize potential replay attacks occurring within the system. The simulation results indicate that the proposed approach provides a more reliable technical means for replay attack detection of such noisy systems, while exhibiting superior adaptability.

Keywords: non-Gaussian noise； unknown but bounded noise； ellipsoid theory； unbiased finite impulse response filtering；replay attack；dynamic threshold

0 引 言

当今信息化社会中, 通信系统的安全问题愈加引发关注, 尤其是重放攻击, 因其不用访问系统内部数据便可对各种通信链路或应用程序进行广泛地攻击[1], 逐步发展为网络安全行业的焦点问题之一. 重放攻击简单易行且难以察觉[2], 是攻击者常用的破坏手段之一, 因此, 研发精准、高效的重放攻击检测技术迫在眉睫.

重放攻击的本质特征在于对合法信息的非授权复用. 攻击者借助非法途径截获合法通信数据后, 通过将其中一个或多个数据重复发送至服务器的方式来诱发多重安全威胁, 包括但不限于通信阻塞、数据篡改以及系统中断等[3]. 针对正常信号与攻击信号的辨识难题, 研究人员相继提出了多种检测技术. 通过考虑动态加密机制[4]、开发加密子系统[5] 和依靠加密调度[6] 等方式, 加密策略在防范重放攻击中取得了

收稿日期: 2025-01-01；**录用日期:** 2025-04-18.

†通信作者. E-mail: lping@ustl.edu.cn.

突出成效, 不过这种模式仍然存在一些无法忽视的缺陷[7], 如加密和解码过程资源的占用问题, 密钥管理的难度以及存储保护等问题. 然而, 面对复杂多变的环境, 系统的安全需求也在持续更新, 此时, 常规的加密技术已经很难满足防护要求. 为此, 学者们尝试引入水印信号[8-9], 在传输数据中嵌入可溯源的合法信息标识, 大幅提升了攻击检测的响应速度. 不过, 水印的嵌入和提取会产生额外的性能损失, 甚至可能会影响原始数据的质量, 导致数据的失真或噪声的增加. 在此背景下, 机器学习凭借其对于时间序列异常变化的卓越感知力[10], 开始成为识别重放攻击行为的重要工具之一. 特别是在智慧城市[11]、电力[12]和车载网络[13] 等智能系统中, 通过持续地训练和优化, 机器学习能够不断地提高对恶意攻击的辨识能力, 为系统安全构筑起动态防御屏障. 但是, 在大规模数据处理时, 机器学习算法可能存在一定的延时性.

值得注意的是, 现阶段的研究大多假设系统噪声是理想的高斯白噪声, 而对于未知噪声系统的讨论屈指可数. 文献 [14] 和文献 [15] 分别建立了未知有界 (unknown but bounded, UBB) 噪声系统的分布式检测方案和齐诺多面体攻击检测系统; 通过分析系统的预测集和估计集, 确认二者是否存在交集, 文献 [16] 成功筛选出重放攻击信号; 通过使用新的切换机制和时变平衡矩阵, 文献 [17] 增加了自由权矩阵的灵活性, 降低了系统的保守性. 但是, 现实中的噪声往往更加复杂, 且可能不是单一噪声, 噪声的性质和强度可能也会随着时间的推移发生波动, 致使经典的静态检测技术在应对这些变化时通常呈现较低的抗干扰性和较弱的灵活性.

为应对这一挑战, 本文聚焦于带有非高斯噪声和 UBB 噪声的系统, 旨在为这类混合噪声系统提供更为精确的重放攻击检测策略. 通过使用权值参数, 结合椭球思想和无偏有限脉冲响应 (unbiased finite impulse response, UFIR) 理论框架, 建立双噪声模型的状态估计器, 采用模型的估计残差来构建重放攻击检测函数, 并设立动态检测阈值, 以修正混合噪声引起的阈值偏差, 避免因阈值选取不当而带来的检测性能下降. 仿真结果显示了所提出方法在复杂噪声环境下的适应性和优越性.

1 系统描述

考虑一个混合噪声系统, 如下所示:

$$\begin{cases} x_{k+1} = \mathcal{A}x_k + \mathcal{B}u_k + w_k + d_k, \\ y_k = \mathcal{C}x_k + v_k + f_k. \end{cases} \tag{1}$$

其中: $x_k \in \mathbb{R}^{N_x}$为系统在k时刻的状态; $u_k \in \mathbb{R}^{N_u}$, $y_k \in \mathbb{R}^{N_y}$分别为系统的控制输入和输出; $\mathcal{A} \in \mathbb{R}^{N_x \times N_x}$, $\mathcal{B} \in \mathbb{R}^{N_x \times N_u}$, $\mathcal{C} \in \mathbb{R}^{N_y \times N_x}$为已知的参数矩阵; d_k和f_k表示均值为 0 的非高斯噪声, 正定矩阵P_k和Q_k分别为d_k和f_k的协方差; w_k和v_k分别为分布未知、边界已知的 UBB 噪声.

假设 1 为构造一个稳定的状态估计器, 假设上述系统是可检测的和可镇定的.

假设 2 系统噪声d_k、f_k、w_k与v_k间相互独立.

2 基于椭球和 UFIR 的状态估计算法

对于系统 (1), 使用 UFIR 滤波技术来处理非高斯噪声, UBB 噪声则借助椭球来描述, 通过二者的融合, 实现对混合噪声系统的状态估计. 系统每次更新时, 先估计下一时刻的状态, 再引进与预测误差成正比的参数项, 对一步预测椭球进行补偿, 最后通过构造一个凸优化问题, 寻求系统状态的最优估计.

2.1 UFIR 滤波算法

当 UBB 噪声$w_k = v_k = 0$时, 系统仅存在随机非高斯噪声, 模型满足 UFIR 滤波条件[18]. 考虑$[m, k]$之间的N个可用量测值, 即$N = k - m + 1$, 将系统模型进行拓展, 如下所示:

$$\begin{cases} X_{m,k} = \mathbb{A}_{m,k}x_{m-1} + \mathbb{B}_{m,k}U_{m,k} + \mathbb{D}_{m,k}\mathcal{D}_{m,k}, \\ Y_{m,k} = \mathbb{C}_{m,k}x_{m-1} + \mathbb{E}_{m,k}U_{m,k} + \\ \qquad \mathbb{F}_{m,k}\mathcal{D}_{m,k} + \mathcal{F}_{m,k}. \end{cases} \tag{2}$$

其中

$$\begin{aligned} X_{m,k} &= [x_m^{\mathrm{T}} \quad x_{m+1}^{\mathrm{T}} \quad \cdots \quad x_k^{\mathrm{T}}]^{\mathrm{T}}, \\ Y_{m,k} &= [y_m^{\mathrm{T}} \quad y_{m+1}^{\mathrm{T}} \quad \cdots \quad y_k^{\mathrm{T}}]^{\mathrm{T}}, \\ U_{m,k} &= [u_{m-1}^{\mathrm{T}} \quad u_m^{\mathrm{T}} \quad \cdots \quad u_{k-1}^{\mathrm{T}}]^{\mathrm{T}}, \\ \mathcal{D}_{m,k} &= [d_{m-1}^{\mathrm{T}} \quad d_m^{\mathrm{T}} \quad \cdots \quad d_{k-1}^{\mathrm{T}}]^{\mathrm{T}} \\ \mathcal{F}_{m,k} &= [f_m^{\mathrm{T}} \quad f_{m+1}^{\mathrm{T}} \quad \cdots \quad f_k^{\mathrm{T}}]^{\mathrm{T}}, \\ \mathbb{A}_{m,k} &= [\mathcal{A}^{\mathrm{T}} \quad \mathcal{A}^{2^{\mathrm{T}}} \quad \cdots \quad \mathcal{A}^{N^{\mathrm{T}}}]^{\mathrm{T}}, \\ \mathbb{B}_{m,k} &= \begin{bmatrix} \mathcal{B} & 0 & \cdots & 0 & 0 \\ \mathcal{A}\mathcal{B} & \mathcal{B} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{A}^{N-2}\mathcal{B} & \mathcal{A}^{N-3}\mathcal{B} & \cdots & \mathcal{B} & 0 \\ \mathcal{A}^{N-1}\mathcal{B} & \mathcal{A}^{N-2}\mathcal{B} & \cdots & \mathcal{A}\mathcal{B} & \mathcal{B} \end{bmatrix}, \\ \mathbb{D}_{m,k} &= \begin{bmatrix} I & 0 & \cdots & 0 & 0 \\ \mathcal{A} & I & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathcal{A}^{N-2} & \mathcal{A}^{N-3} & \cdots & I & 0 \\ \mathcal{A}^{N-1} & \mathcal{A}^{N-2} & \cdots & \mathcal{A} & I \end{bmatrix}, \\ \mathbb{C}_{m,k} &= \mathrm{diag}[\mathcal{C} \quad \mathcal{C} \quad \cdots \quad \mathcal{C}]\mathbb{A}_{m,k}, \\ \mathbb{E}_{m,k} &= \mathrm{diag}[\mathcal{C} \quad \mathcal{C} \quad \cdots \quad \mathcal{C}]\mathbb{B}_{m,k}, \\ \mathbb{F}_{m,k} &= \mathrm{diag}[\mathcal{C} \quad \mathcal{C} \quad \cdots \quad \mathcal{C}]\mathbb{D}_{m,k}. \end{aligned}$$

批处理的窗口大小与模型的状态维度N_x相等. 在$n = m + N_x - 1$时, 广义噪声功率增益G_n以及

迭代的系统状态$\hat{x}_n$[19]分别为

$$\begin{cases} G_n = (\mathcal{H}_{m,n}^{\mathrm{T}}\mathcal{H}_{m,n})^{-1}, \\ \hat{x}_n = (\mathcal{H}_{m,n}^{\mathrm{T}}\mathcal{H}_{m,n})^{-1}\mathcal{H}_{m,n}^{\mathrm{T}}(Y_{m,n} - \mathbb{E}_{m,n}U_{m,n}) + \\ \quad\ \mathbb{B}_{m,n}^{(N_x)}U_{m,n}. \end{cases} \tag{3}$$

其中: $\mathbb{B}_{m,n}^{(N_x)}$为$\mathbb{B}_{m,n}$的第N_x行, 而

$$\mathcal{H}_{m,k} = \begin{bmatrix} \mathcal{C}(\mathcal{A}^{N-1})^{-1} & \mathcal{C}(\mathcal{A}^{N-2})^{-1} & \cdots & \mathcal{C}\mathcal{A}^{-1} & \mathcal{C} \end{bmatrix}^{\mathrm{T}}.$$

UFIR 滤波器从第l时刻开始更新迭代, $l = m + N_x$, 持续至第k时刻. 根据批处理获得的初始值, 运用下式[20]进行迭代更新:

$$\begin{cases} \hat{x}_{l|l-1} = \mathcal{A}\hat{x}_{l-1|l-1} + \mathcal{B}u_l, \\ \hat{x}_{l|l} = \hat{x}_{l|l-1} + G_l\mathcal{C}^{\mathrm{T}}(y_l - \mathcal{C}\hat{x}_{l|l-1}), \\ G_l = [\mathcal{C}^{\mathrm{T}}\mathcal{C} + (\mathcal{A}G_{l-1}\mathcal{A}^{\mathrm{T}})^{-1}]^{-1}. \end{cases} \tag{4}$$

其中: $\hat{x}_{l|l-1}$为l时刻的先验估计, $\hat{x}_{l|l}$为l时刻的后验估计.

2.2　状态估计

定义 1　椭球集合$\Omega(\hat{x}, \mathcal{M})$可由下式[21]表示:

$$\Omega(\hat{x}, \mathcal{M}) = \{x : (x - \hat{x})^{\mathrm{T}}\mathcal{M}^{-1}(x - \hat{x}) \leqslant 1\}.$$

其中: $\hat{x}$为椭球中心; 正定对称矩阵$\mathcal{M}$表示椭球的形状矩阵, 界定了椭球向每个角度延伸的距离.

引理 1　对于椭球$\Omega(x, \mathcal{M})$中的任一个元素进行$\tilde{x} = Dx + F$的线性映射, 可得到如下新椭球集[22]:

$$D\Omega(x, \mathcal{M}) + F = \Omega(Dx + F, D\mathcal{M}D^{\mathrm{T}}),$$

其中D和F分别为已知的矩阵以及向量.

引理 2　给定M个椭球$\Omega_i(x_i, \mathcal{M}_i)(i = 1, 2, \ldots, M)$的闵可夫斯基和运算[23]为

$$\Omega_1(x_1, \mathcal{M}_1) \oplus \ldots \oplus \Omega_N(x_N, \mathcal{M}_N) \subseteq \Omega_N(x, \mathcal{M}).$$

其中: $x = \sum_{i=1}^{M} x_i$, $\mathcal{M} = \sum_{i=1}^{M} \frac{1}{\sigma_i}\mathcal{M}_i$, $\sigma_i > 0$且$\sum_{i=1}^{M} \sigma_i = 1$.

假设 3　UBB 噪声w_k和v_k分别满足椭球集合

$$\Omega_w = \{w_k : w_k^{\mathrm{T}}(\mathcal{M}_k^w)^{-1}w_k \leqslant 1\},$$
$$\Omega_v = \{v_k : v_k^{\mathrm{T}}(\mathcal{M}_k^v)^{-1}v_k \leqslant 1\}.$$

假设系统初始时刻的状态为x_0, 初始后验估计满足$\hat{x}_{0|0} = x_0$. 本节利用时间更新和测量更新这两个环节, 描述了第$k-1$时刻到第k时刻的状态估计过程: 下面的定理 1 给出了时间更新的详细推导, 预测第k时刻的先验估计; 定理 2 则根据第k时刻的观测值更新系统的状态后验估计.

由于系统 (1) 同时受到非高斯噪声和 UBB 噪声的影响, 在$k-1$时刻系统状态的后验估计可表示为一个点估计与两个混合噪声分量的和的形式, 即

$$\hat{x}_{k-1|k-1} = \hat{x}_{k-1|k-1}^c + \alpha_{k-1|k-1} + \beta_{k-1|k-1}. \tag{5}$$

其中: $\hat{x}_{k-1|k-1}^c$为点估计值, 即系统未受到噪声干扰时的状态后验估计; $\alpha_{k-1|k-1} \in \Omega(0, \mathcal{M}_{k-1|k-1}^{\alpha})$表示中心为原点, 形状矩阵为$\mathcal{M}_{k-1|k-1}^{\alpha}$的椭球; $\beta_{k-1|k-1}$表示均值为 0, 协方差矩阵为$\mathcal{Q}_{k-1|k-1}$的非高斯噪声. 系统下一时刻的先验估计为

$$\hat{x}_{k|k-1} = \mathcal{A}\hat{x}_{k-1|k-1} + \mathcal{B}u_{k-1} + w_{k-1} + d_{k-1}. \tag{6}$$

定理 1　对于混合噪声系统 (1), k时刻的状态先验估计$\hat{x}_{k|k-1}$可描述为

$$\hat{x}_{k|k-1} = \hat{x}_{k|k-1}^c + \alpha_{k|k-1} + \beta_{k|k-1}. \tag{7}$$

其中: $\hat{x}_{k|k-1}^c = \mathcal{A}\hat{x}_{k-1|k-1}^c + \mathcal{B}u_{k-1}$; 非高斯噪声$\beta_{k|k-1}$的均值为 0, 协方差为$\mathcal{Q}_{k|k-1} = \mathcal{A}\mathcal{Q}_{k-1|k-1}\mathcal{A}^{\mathrm{T}} + P_{k-1}$; UBB 噪声$\alpha_{k|k-1} \in \Omega(0, \mathcal{M}_{k|k-1}^{\alpha})$, 其形状矩阵满足

$$\mathcal{M}_{k|k-1}^{\alpha} = (\sqrt{\mathrm{tr}(\mathcal{A}\mathcal{M}_{k-1|k-1}^{\alpha}\mathcal{A}^{\mathrm{T}})} + \sqrt{\mathrm{tr}(\mathcal{M}_{k-1}^{w})})\times \left(\frac{\mathcal{A}\mathcal{M}_{k-1|k-1}^{\alpha}\mathcal{A}^{\mathrm{T}}}{\sqrt{\mathrm{tr}(\mathcal{A}\mathcal{M}_{k-1|k-1}^{\alpha}\mathcal{A}^{\mathrm{T}})}} + \frac{\mathcal{M}_{k-1}^{w}}{\sqrt{\mathrm{tr}(\mathcal{M}_{k-1}^{w})}}\right).$$

证明　将式 (5) 代入 (6), 可知

$$\begin{aligned} \hat{x}_{k|k-1} &= \mathcal{A}(\hat{x}_{k-1|k-1}^c + \alpha_{k-1|k-1} + \beta_{k-1|k-1}) + \\ &\quad \mathcal{B}u_{k-1} + w_{k-1} + d_{k-1} = \\ &\quad \hat{x}_{k|k-1}^c + \alpha_{k|k-1} + \beta_{k|k-1}. \end{aligned} \tag{8}$$

其中: $\hat{x}_{k|k-1}^c = \mathcal{A}\hat{x}_{k-1|k-1}^c + \mathcal{B}u_{k-1}$, $\alpha_{k|k-1} = w_{k-1} + \mathcal{A}\alpha_{k-1|k-1}$, $\beta_{k|k-1} = d_{k-1} + \mathcal{A}\beta_{k-1|k-1}$. 由引理 1 和最小迹椭球法, 可得到

$$\alpha_{k|k-1} \in \Omega(0, \mathcal{M}_{k|k-1}^{\alpha}), \tag{9}$$

这里

$$\mathcal{M}_{k|k-1}^{\alpha} = (\sqrt{\mathrm{tr}(\mathcal{A}\mathcal{M}_{k-1|k-1}^{\alpha}\mathcal{A}^{\mathrm{T}})} + \sqrt{\mathrm{tr}(\mathcal{M}_{k-1}^{w})})\times \left(\frac{\mathcal{A}\mathcal{M}_{k-1|k-1}^{\alpha}\mathcal{A}^{\mathrm{T}}}{\sqrt{\mathrm{tr}(\mathcal{A}\mathcal{M}_{k-1|k-1}^{\alpha}\mathcal{A}^{\mathrm{T}})}} + \frac{\mathcal{M}_{k-1}^{w}}{\sqrt{\mathrm{tr}(\mathcal{M}_{k-1}^{w})}}\right).$$

d_{k-1}与$\beta_{k-1|k-1}$相互独立, 故

$$\mathrm{E}[\beta_{k|k-1}] = \mathrm{E}[d_{k-1} + \mathcal{A}\beta_{k-1|k-1}] = 0, \tag{10}$$

$$\mathcal{Q}_{k|k-1} = \mathrm{cov}[\beta_{k|k-1}] = \mathcal{A}\mathcal{Q}_{k-1|k-1}\mathcal{A}^{\mathrm{T}} + P_{k-1}. \tag{11}$$

证毕. □

利用y_k对一步预测椭球实施误差补偿, 系统的后验估计可描述为

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + G_k\mathcal{C}^{\mathrm{T}}(y_k - \mathcal{C}\hat{x}_{k|k-1}). \tag{12}$$

定理 2　对于系统 (1), 存在正标量ς_k, 使得k时刻的后验估计为

$$\hat{x}_{k|k}=\hat{x}^c_{k|k}+\alpha_{k|k}+\beta_{k|k}. \tag{13}$$

其中: $\hat{x}^c_{k|k}=(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\hat{x}^c_{k|k-1}+G_k\mathcal{C}^{\mathrm{T}}y_k$; UBB 噪声$\alpha_{k|k}\in\Omega(0,\mathcal{M}^{\alpha}_{k|k})$, 其形状矩阵为

$$\begin{aligned}&\mathcal{M}^{\alpha}_{k|k}=\\&(\varsigma_k+1)(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{M}^{\alpha}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}}+\\&\Big(1+\frac{1}{\varsigma_k}\Big)G_k\mathcal{C}^{\mathrm{T}}\mathcal{M}^{v}_{k}\mathcal{C}G^{\mathrm{T}}_k;\end{aligned}$$

非高斯噪声$\beta_{k|k}$的均值为 0, 协方差矩阵为

$$\begin{aligned}&\mathcal{Q}_{k|k}=\\&(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{Q}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}}+G_k\mathcal{C}^{\mathrm{T}}Q_k\mathcal{C}G^{\mathrm{T}}_k.\end{aligned}$$

证明 将式 (7) 代入 (12), 可得到

$$\begin{aligned}\hat{x}_{k|k}=&\hat{x}^c_{k|k-1}+\alpha_{k|k-1}+\beta_{k|k-1}+\\&G_k\mathcal{C}^{\mathrm{T}}(y_k-\mathcal{C}(\hat{x}^c_{k|k-1}+\alpha_{k|k-1}+\beta_{k|k-1}))=\\&\hat{x}^c_{k|k}+\alpha_{k|k}+\beta_{k|k}.\end{aligned} \tag{14}$$

其中

$$\begin{aligned}\hat{x}^c_{k|k}&=(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\hat{x}^c_{k|k-1}+G_k\mathcal{C}^{\mathrm{T}}\mathcal{C}x_k,\\\alpha_{k|k}&=(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\alpha_{k|k-1}+G_k\mathcal{C}^{\mathrm{T}}v_k,\\\beta_{k|k}&=(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\beta_{k|k-1}+G_k\mathcal{C}^{\mathrm{T}}f_k.\end{aligned}$$

对于系统状态后验估计的点估计部分, 有$v_k=f_k=0$, 故

$$\hat{x}^c_{k|k}=(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\hat{x}^c_{k|k-1}+G_k\mathcal{C}^{\mathrm{T}}y_k. \tag{15}$$

又因$v_k\in\Omega(0,\mathcal{M}^{v}_{k})$和$\alpha_{k|k-1}\in\Omega(0,\mathcal{M}^{\alpha}_{k|k-1})$, 可得到

$$\begin{aligned}\alpha_{k|k}=&\Omega(0,(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{M}^{\alpha}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}})\oplus\\&\Omega(0,G_k\mathcal{C}^{\mathrm{T}}\mathcal{M}^{v}_{k}\mathcal{C}G^{\mathrm{T}}_k)\subseteq\\&\Omega(0,\mathcal{M}^{\alpha}_{k|k}),\end{aligned} \tag{16}$$

这里$\mathcal{M}^{\alpha}_{k|k}=\dfrac{1}{\sigma_1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{M}^{\alpha}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}}+\dfrac{1}{\sigma_2}G_k\mathcal{C}^{\mathrm{T}}\mathcal{M}^{v}_{k}\mathcal{C}G^{\mathrm{T}}_k$. 由引理 2 可知$\sigma_1+\sigma_2=1$, 令$\sigma_1=\dfrac{1}{\varsigma_k+1}$, $\sigma_2=\dfrac{\varsigma_k}{\varsigma_k+1}$, ς_k为任意正实数. 则$\mathcal{M}^{\alpha}_{k|k}$可改写为

$$\begin{aligned}\mathcal{M}^{\alpha}_{k|k}=&(\varsigma_k+1)(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{M}^{\alpha}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}}+\\&\Big(1+\frac{1}{\varsigma_k}\Big)G_k\mathcal{C}^{\mathrm{T}}\mathcal{M}^{v}_{k}\mathcal{C}G^{\mathrm{T}}_k.\end{aligned} \tag{17}$$

$\beta_{k|k}$的均值和协方差矩阵分别为

$$\mathrm{E}[\beta_{k|k}]=\mathrm{E}[(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\beta_{k|k-1}+G_k\mathcal{C}^{\mathrm{T}}f_k]=0, \tag{18}$$

$$\begin{aligned}&\mathcal{Q}_{k|k}=\mathrm{cov}[\beta_{k|k}]=\\&(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{Q}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}}+G_k\mathcal{C}^{\mathrm{T}}Q_k\mathcal{C}G^{\mathrm{T}}_k.\end{aligned} \tag{19}$$

证毕. □

后验估计的均方误差涉及混合噪声, 为求解得到使得均方误差最小的增益因子和参数ς_k, 引入权值因子$\mu\in[0,1]$来构建一个多目标优化准则, 有

$$J(\varsigma_k)=\mu\mathrm{tr}(\mathcal{Q}_{k|k})+(1-\mu)\mathrm{tr}(\mathcal{M}^{\alpha}_{k|k}). \tag{20}$$

将$\mathcal{Q}_{k|k}$和$\mathcal{M}^{\alpha}_{k|k}$代入目标函数 (20), 有

$$\begin{aligned}&J(\varsigma_k)=\\&\mu\mathrm{tr}((I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{Q}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}})+\\&\mu\mathrm{tr}(G_k\mathcal{C}^{\mathrm{T}}Q_k\mathcal{C}G^{\mathrm{T}}_k)+(1-\mu)(\varsigma_k+1)\times\\&\mathrm{tr}((I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{M}^{\alpha}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}})+\\&(1-\mu)\Big(1+\frac{1}{\varsigma_k}\Big)\mathrm{tr}(G_k\mathcal{C}^{\mathrm{T}}\mathcal{M}^{v}_{k}\mathcal{C}G^{\mathrm{T}}_k).\end{aligned} \tag{21}$$

令$\mathcal{T}=\mathrm{tr}((I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{M}^{\alpha}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}})$, $\mathcal{Z}=\mathrm{tr}(G_k\mathcal{C}^{\mathrm{T}}\mathcal{M}^{v}_{k}\mathcal{C}G^{\mathrm{T}}_k)$. 当且仅当$\varsigma_k=\sqrt{\dfrac{\mathcal{Z}}{\mathcal{T}}}$时$J(\varsigma_k)$的值最小, 即

$$\begin{aligned}&\min J(\varsigma_k)=\\&\mu\mathrm{tr}((I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{Q}_{k|k-1}(I-G_k\mathcal{C}^{\mathrm{T}}\mathcal{C})^{\mathrm{T}})+\\&\mu\mathrm{tr}(G_k\mathcal{C}^{\mathrm{T}}Q_k\mathcal{C}G^{\mathrm{T}}_k)+(1-\mu)(\sqrt{\mathcal{T}}+\sqrt{\mathcal{Z}})^2.\end{aligned} \tag{22}$$

令$J(\varsigma_k)$进行关于G_k的微分方程等于 0 来获取最优增益, 有

$$\begin{aligned}&G^*_k=\\&(\mu\mathcal{Q}_{k|k-1}\mathcal{C}^{\mathrm{T}}\mathcal{C}+(1-\mu)(\varsigma_k+1)\mathcal{M}^{\alpha}_{k|k-1}\mathcal{C}^{\mathrm{T}}\mathcal{C})\mathcal{K}^{-1},\end{aligned} \tag{23}$$

其中

$$\begin{aligned}\mathcal{K}=&\mathcal{C}^{\mathrm{T}}\mathcal{C}(\mu\mathcal{Q}_{k|k-1}+(1-\mu)(\varsigma_k+1)\mathcal{M}^{\alpha}_{k|k-1})\mathcal{C}^{\mathrm{T}}\mathcal{C}+\\&\mathcal{C}^{\mathrm{T}}\Big(\mu Q_k+(1-\mu)\Big(1+\frac{1}{\varsigma_k}\Big)\mathcal{M}^{v}_{k}\Big)\mathcal{C}.\end{aligned}$$

将G^*_k代入式 (22), 对下式中的最小化问题进行求取, 即可获得ς_k的最优解:

$$\begin{aligned}&\min_{\varsigma_k}J(\varsigma_k);\\&\mathrm{s.t.}\ \varsigma_k>0,\\&\quad\varsigma_k\in\mathbb{R}^1.\end{aligned} \tag{24}$$

由于目标函数$J(\varsigma_k)$是凸函数且定义在凸集上, 其局部极小值即为全局极小值. 鉴于此, 可依托 Matlab 工具箱来计算上述最优值, 然后, 利用增益矩阵G_k与参数ς_k的最优解便可推导出系统的后验估计$\hat{x}_{k|k}$, 在长期稳定状态下, 增益G_k会逐渐趋于一个稳态值G.

3 重放攻击检测机制

开展重放攻击的过程主要包括监听、窃取和重播. 攻击者通过网络嗅探等隐蔽手段非法监听目标系统的通信流, 对数据进行解析和记录, 然后择机进行信息回输, 完成对控制指令的恶意操作[24]. 本文利用模型的残差值建立检测信号, 捕捉被攻击时刻的残差分布, 以实现对重放攻击的检测. 为便于计算,

假设攻击者在$k=1$时刻开始释放截取的历史合法信息, 考虑k时刻系统的残差为$r_k=y_k-\mathcal{C}\hat{x}_{k|k}$. 攻击检测函数$\xi_k$可描述为

$$\xi_k=\frac{1}{t}\sum_{i=k-t+1}^{k}r_k^{\mathrm{T}}r_k, \tag{25}$$

其中t为窗口大小. 建立重放攻击检测规则为

$$\begin{cases}\xi_k>\theta_k, \text{ 受到重放攻击;}\\ \xi_k\leqslant\theta_k, \text{ 运行正常.}\end{cases} \tag{26}$$

这里θ_k为检测阈值. 目前, 大部分检测技术中, 阈值普遍选用$\theta_k=\sup\|r_k\|$, 但是, 非高斯噪声的自身特性常导致残差易出现突发性波动, 使得阈值选取难以兼顾灵敏度与鲁棒性. 为解决这一问题, 引入滑动窗口τ来动态计算检测阈值θ_k, 在每个时刻计算窗口内ξ_k的均值$\Im_k$和标准差Λ_k, 有

$$\begin{cases}\Im_k=\dfrac{1}{\tau}\displaystyle\sum_{i=k-\tau+1}^{k}\xi_i,\\ \Lambda_k=\sqrt{\dfrac{1}{\tau-1}\displaystyle\sum_{i=k-\tau+1}^{k}(\xi_i-\Im_k)^2}.\end{cases} \tag{27}$$

检测阈值θ_k可描述为

$$\theta_k=\bar{\Im}_k+\eta\bar{\Lambda}_k. \tag{28}$$

其中: η为常数, 通常取$\eta=2$或3, 对应 95% 或 99.7% 的置信区间. 为防止每个时刻的微小振荡对阈值造成干扰, 设置$\iota\,(\iota>0)$为阈值变化的最小变化幅度, 只有$|\theta_k-\theta_{k-1}|\geqslant\iota$时, 才会更新$\theta_k$; 否则, 保持不变. 通过这种在线调整, 系统可以更好地应对混合噪声多模态特性, 增加自身的鲁棒性, 在面对重放攻击促使数据突变时, 这种动态更新也有利于系统及时捕获异常信号, 极大降低了因θ_k失配而引发的误报和漏报行为.

假设发生重放攻击时的模型残差为r_k^a, 对应的输出变量和状态后验估计分别为y_k^a和$\hat{x}_{k|k}^a$, k时刻系统的实际残差r_k^*为

$$r_k^*=y_k^a-\mathcal{C}\hat{x}_{k|k}=r_k^a+\mathcal{C}(\hat{x}_{k|k}^a-\hat{x}_{k|k}). \tag{29}$$

运用 LQG 控制器来获取最佳控制律u_k, 假设L为系统平稳运转时的反馈矩阵, 可知$u_k=L\hat{x}_{k|k}$. 第k时刻攻击者已将系统的输出y_k替换为y_k^a, 故

$$\begin{aligned}&\hat{x}_{k|k}^a-\hat{x}_{k|k}=\\&\hat{x}_{k|k}^{a,c}-\hat{x}_{k|k}^c+\Delta\alpha_{k|k}+\Delta\beta_{k|k}=\\&\sum_{i=0}^{k-1}\phi^i\mathcal{B}L(\Delta\alpha_{k-i-1|k}+\Delta\beta_{k-i-1|k})+\\&\phi^k(\hat{x}_{0|0}^{a,c}-\hat{x}_{0|0}^c)+\Delta\alpha_{k|k}+\Delta\beta_{k|k}.\end{aligned} \tag{30}$$

其中: $\Delta\alpha_{k|k}=\alpha_{k|k}^a-\alpha_{k|k}$, $\Delta\beta_{k|k}=\beta_{k|k}^a-\beta_{k|k}$, 分别为$k$时刻重放的不同噪声信号与其对应的正常噪声信号的差; $\phi=(I-G\mathcal{C}^{\mathrm{T}}\mathcal{C})(\mathcal{A}+\mathcal{B}L)$. 在系统稳定的前提下, 式 (30) 最后一个等号右侧第 1 项收敛至 0, 攻击时的实际检测函数为

$$\begin{aligned}&\xi_k^*=\frac{1}{t}\sum_{i=k-t+1}^{k}r_k^{*\mathrm{T}}r_k^*=\\&\frac{1}{t}\sum_{i=k-t+1}^{k}\Big(r_k^a+\mathcal{C}\Big(\sum_{i=0}^{k-1}\phi^i\mathcal{B}L(\Delta\alpha_{k-i-1|k}+\\&\Delta\beta_{k-i-1|k})+\Delta\alpha_{k|k}+\Delta\beta_{k|k}\Big)\Big)^{\mathrm{T}}\times\\&\Big(r_k^a+\mathcal{C}\Big(\sum_{i=0}^{k-1}\phi^i\mathcal{B}L(\Delta\alpha_{k-i-1|k}+\Delta\beta_{k-i-1|k})+\\&\Delta\alpha_{k|k}+\Delta\beta_{k|k}\Big)\Big)=\\&\xi_k^a+\frac{1}{t}\sum_{i=k-t+1}^{k}\Big\|\mathcal{C}\Big(\sum_{i=0}^{k-1}\phi^i\mathcal{B}L(\Delta\alpha_{k-i-1|k}+\\&\Delta\beta_{k-i-1|k})+\Delta\alpha_{k|k}+\Delta\beta_{k|k}\Big)\Big\|_2^2.\end{aligned} \tag{31}$$

这里: $\|\cdot\|_2$为向量的 2 范数; ξ_k^a为重新注入系统的历史合法信息所对应的检测函数, 故ξ_k^a在检测阈值内, 而系统每个时刻的非高斯噪声和 UBB 噪声均是随机产生, 因此噪声差值不会总为 0, 式 (31) 最后一个等号右侧第 2 项便不会收敛至 0, 此时的检测函数ξ_k^*大于正常的检测阈值, 换言之, 系统 (1) 可能会遇到的重放攻击在所提出方案下具有可检测性.

4 仿　真

为验证所提出算法的可行性, 考虑双容水箱的非线性系统模型, 其动力学方程为

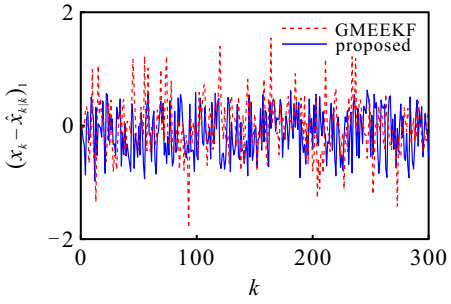
$$\begin{aligned}\varepsilon_1\frac{\mathrm{d}\mathcal{L}_1}{\mathrm{d}t}&=q_1-q_2,\\ \varepsilon_2\frac{\mathrm{d}\mathcal{L}_2}{\mathrm{d}t}&=q_2-q_3.\end{aligned}$$

其中: ε为容量系数; $\mathcal{L}$为水箱的液位; 液体流入量q_1与水泵的电压$\mathcal{V}$以及流量系数ℓ相关, 即$q_1=\ell\mathcal{V}$; $q_2=\mathcal{S}_1\sqrt{2g(\mathcal{L}_1-\mathcal{L}_2)}$和$q_3=\mathcal{S}_2\sqrt{2g\mathcal{L}_2}$分别为两个水箱的液体流出量, $\mathcal{S}$为液体流出时的横截面积. 采样周期设为 0.15 s, 对模型的动力学方程离散化, 可得到系统参数$\mathcal{A}=\begin{bmatrix}1&-0.1\\0.1&0.9\end{bmatrix}$, $\mathcal{B}=\begin{bmatrix}0.7\\0.3\end{bmatrix}$, $\mathcal{C}=\begin{bmatrix}1&0.2\\-0.3&0.789\end{bmatrix}$.

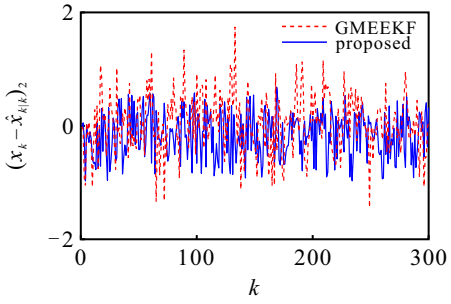
为全面评估所提出策略在重放攻击下的性能, 首先, 模拟攻击者截取$k=50\sim100$ s的信息. 然后, 分两种情形展开攻击: 1) 下一秒立即开始重播, 直至第 180 s 停止; 2) 间隔一段时间后, 在$k=250\sim300$ s

内将复制的数据进行重放. 最后, 在 3 种不同的噪声情境下进行仿真测试, 分别为仅非高斯噪声、仅 UBB 噪声以及两者并存的情况.

1) 仅非高斯噪声. 本场景仅考虑系统噪声服从非高斯统计特性的情况, 这类噪声常具有不对称或尾部较重等特点. 由于不包含 UBB 噪声, 设置$\mu=1$, 噪声w_k和v_k、形状矩阵$\mathcal{M}_0^w$和$\mathcal{M}_0^v$分别为对应的零向量或零矩阵, $P_0=Q_0=\mathrm{diag}[0.2\quad 0.2]$, $\iota=0.3$, $\tau=20$, $\eta=2$. 图 1 为所设计方案与基于广义最小误差熵的卡尔曼滤波 (Kalman filter based on the generalized minimum error entropy, GMEEKF) 算法[25] 的状态估计误差对比.



(a) 非高斯噪声下状态估计误差 $(x_k-\hat{x}_{k|k})_1$



(b) 非高斯噪声下状态估计误差 $(x_k-\hat{x}_{k|k})_2$

图1 非高斯噪声下的状态估计误差

由图 1 可见, 尽管误差波动水平大致接近, 但是, GMEEKF 算法出现了多次明显的陡升和陡降现象, 所提出方法的最大误差峰值较 GMEEKF 算法降低了 46.28% 左右, 误差变化更小, 突显其对非高斯噪声异常值的强抑制力.

图 2 为不同攻击场景下的重放攻击检测效果.

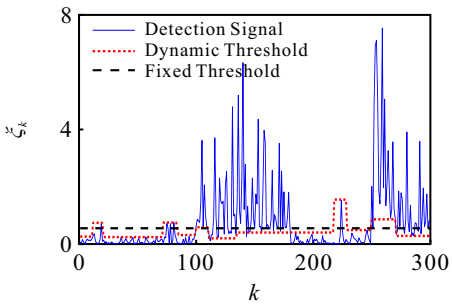
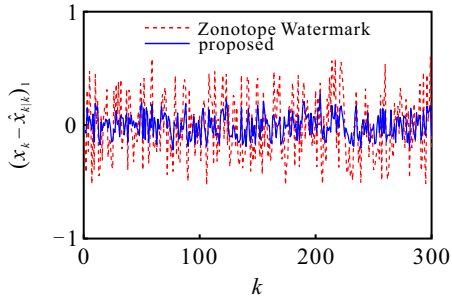


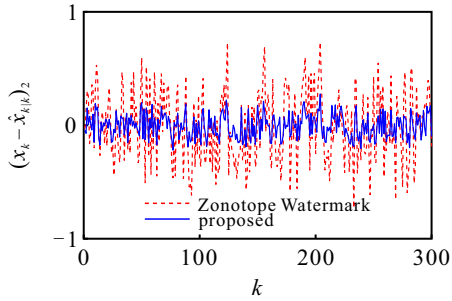
图2 非高斯噪声下的重放攻击检测

由图 2 可见, 对于非高斯噪声系统, 所提出检测系统能够有效地分辨攻击信号与背景噪声间的差异性, 相比之下, 固定阈值频繁与检测曲线交叉, 导致大量误判和漏报.

2) 仅 UBB 噪声. UBB 噪声w_k、v_k满足$w_0\in\Omega(0,\mathcal{M}_0^w)$和 $w_0\in\Omega(0,\mathcal{M}_0^v)$, 设置 $\mathcal{M}_0^w=\mathcal{M}_0^v=\mathrm{diag}[0.5\quad 0.5]$, $\iota=0.1$, $\tau=15$, $\eta=2$, 考虑不存在非高斯噪声, 故$\mu=0$, 噪声d_k和f_k、协方差P_0和Q_0分别为相对应的零向量或零矩阵. 针对单一 UBB 噪声场景, 基于状态估计误差和重放攻击检测的双度量准则, 构建与文献 [26] Zonotope 水印法中案例 1 的对比实验, 如图 3 所示.



(a) UBB 噪声下状态估计误差 $(x_k-\hat{x}_{k|k})_1$



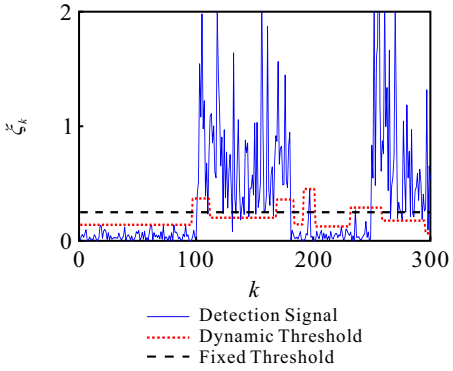
(b) UBB 噪声下状态估计误差 $(x_k-\hat{x}_{k|k})_2$

图3 UBB 噪声下的状态估计误差

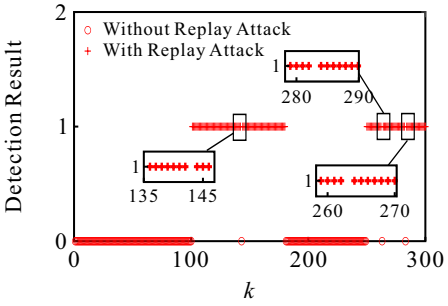
图 3 的误差分析表明: Zonotope 水印法的误差表现出较强的非平稳特性; 与之形成鲜明对比的是, 所提出算法各时段的误差值均能够维持在相对稳定的区间范围内, 最大误差峰值降低了约 62.33%.

图 4 和图 5 分别从不同维度揭示了算法的检测性能. 图 4 为随机的单次检测结果. 其中: Zonotope 水印法中的“1”表示重放攻击发生, “0”表示未发生攻击. 由图 4 中数据可知, 所提出算法的检测率仅比 Zonotope 水印法高出 0.67%. 为消除单次实验的偶然性, 本文进行了 120 次的独立随机实验, 通过绘制平均检测率曲线来进一步得到更具统计意义的性能评估, 如图 5 所示. 由图 5 可见: 初期 (前 25 次) 两条曲线均存在较大幅度的抖动; 当进入稳定期 (58 次后), 所提出机制的平均检测率稳定在 99.23% 左右,

优于 Zonotope 水印法的 97.47%, 这种差距表明了所提出算法在不同批次的实验中均能够保障高水准的检测力, 验证了其长期运行的可靠性.



(a) UBB 噪声下本文方法检测结果



(b) UBB 噪声下Zonotope 水印法检测结果

图4　UBB 噪声下的重放攻击检测

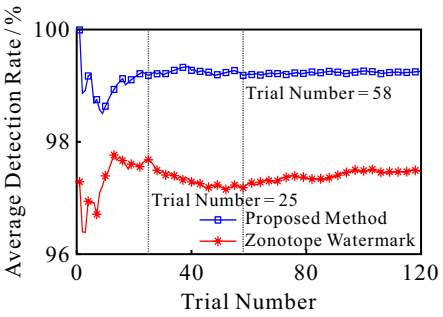


图5　UBB 噪声下两种算法的平均检测率

3) 非高斯噪声和 UBB 噪声. 假设在该场景中, 非高斯噪声和 UBB 噪声共同作用, 设置 $P_0 = Q_0 = \mathrm{diag}[0.2 \quad 0.2]$, $\mu = 0.5$, ι=0.3, $\tau = 25$, $\eta = 2$, $\mathcal{M}_0^w = \mathcal{M}_0^v = \mathrm{diag}[0.5 \quad 0.5]$. 图 6 为混合噪声下状态估计误差的 PDF 分布. 图 6 中状态估计误差的概率密度函数 (probability density function, PDF) 以非对称的形态分布, 表明了误差在不同维度上的异质特征, 体现了算法对于不同噪声源的降噪能力; 多峰结构的稀疏化特征表明了算法能够充分抑制噪声叠加效应, 进而在保证估计精度的前提下, 显著降低了攻击检测的误判率. 图 7 为混合噪声下的重放攻击检测. 由图 7 的检测曲线可知: 无重放攻击时, 动态检测阈值在信号平缓区保持恒定, 在振荡区则根据波动情况自适应调整, 从而避免将强干扰误判为攻击; 当重放攻击发生时, 检测信号瞬间增大, 并迅速突破阈值, 在攻击持续阶段, 阈值线产生适应性偏移, 但是检测曲线仍然处于阈值之上, 直至恶意攻击消失, 这一过程反映了系统对于不同重放攻击的高敏感性.

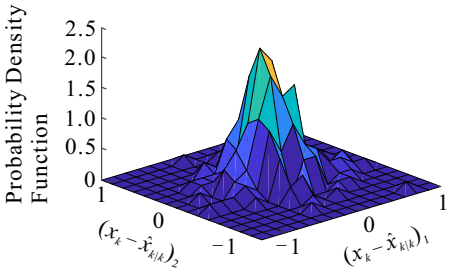


图6　混合噪声下状态估计误差的 PDF 分布

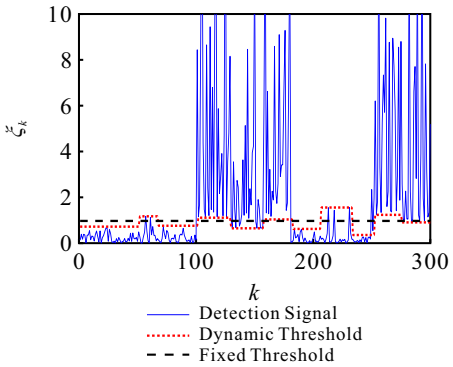


图7　混合噪声下的重放攻击检测

5　结　论

与以往局限于单一噪声源的方法不同, 本文设计了一种适用于非高斯噪声和 UBB 噪声共存场景的重放攻击检测算法. 借助权值因子, 通过优化噪声建模以及状态更新过程, 搭建了一种融合椭球算法和 UFIR 滤波的新型状态估计器, 使得系统模型的估计精度得到了明显提升. 在每个时刻, 充分分析系统观测值与估计值间的偏差, 提出了一种准确识别重放攻击的检测函数, 并设计了检测阈值的自动调节机制. 该机制可灵活地利用历史和当前检测信号来调整阈值, 增强了对潜在重放攻击的检测能力. 实验结果表明, 即便在复杂的混合噪声系统中, 所构建检测技术依然具有较高的准确度和较好的稳定性.

参考文献 (References)

[1] 叶丹, 靳凯净, 张天予. 网络攻击下的信息物理系统安全性研究综述[J]. 控制与决策, 2023, 38(8): 2243-2252. (Ye D, Jin K J, Zhang T Y. A survey on security of cyber-physical systems under network attacks[J]. Control and Decision, 2023, 38(8): 2243-2252.)

[2] Zhang Z D, Li M D, Xie L B. Data-driven replay attack detection for unknown cyber-physical systems[J]. Information Sciences, 2024, 670: 120562.

[3] 宋金波, 董宏丽, 申雨轩, 等. 重放攻击下多智能体系统H_∞一致性PID控制[J]. 控制理论与应用, 2024, 41(4): 658-666.
(Song J B, Dong H L, Shen Y X, et al. H_∞-consensus PID control of multi-agent systems under replay attack[J]. Control Theory & Applications, 2024, 41(4): 658-666.)

[4] Li T X, Wang Z D, Zou L, et al. A dynamic encryption-decryption scheme for replay attack detection in cyber-physical systems[J]. Automatica, 2023, 151: 110926.

[5] Rasheed A, Baza M, Badr M M, et al. Efficient crypto engine for authenticated encryption, data traceability, and replay attack detection over CAN bus network[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(1): 1008-1025.

[6] Song Y B, Ye D. Replay attack detection and mitigation for cyber-physical systems via RADIR algorithm with encryption scheduling[J]. Neurocomputing, 2023, 558: 126698.

[7] Li T X, Weng P D, Chen B, et al. Encryption-based attack detection scheme for multisensor secure fusion estimation[J]. IEEE Transactions on Aerospace and Electronic Systems, 2024, 60(5): 7548-7554.

[8] 张正道, 王瑶瑶, 谢林柏. 基于伪周期控制信号编码的重放攻击检测[J]. 控制与决策, 2023, 38(10): 2962-2968.
(Zhang Z D, Wang Y Y, Xie L B. Replay attack detection method based on pseudo periodic control signal coding[J]. Control and Decision, 2023, 38(10): 2962-2968.)

[9] Jia S Y, Guo Q L. A dynamic-watermarking-based cyberattack detection framework on an LFC system with uncertain parameters[J]. IEEE Internet of Things Journal, 2024, 11(14): 24389-24399.

[10] 李康, 李爽, 高小永, 等. 多变量时序标记Transformer及其在电潜泵故障诊断中的应用[J]. 控制与决策, 2025, 40(4): 1145-1153.
(Li K, Li S, Gao X Y, et al. Multivariate time series tokenized Transformer and its application in fault diagnosis of electric submersible pump[J]. Control and Decision, 2025, 40(4): 1145-1153.)

[11] Elsaeidy A A, Jagannath N, Sanchis A G, et al. Replay attack detection in smart cities using deep learning[J]. IEEE Access, 2020, 8: 137825-137837.

[12] Khaw Y M, Jahromi A A, Arani M F M, et al. A deep learning-based cyberattack detection system for transmission protective relays[J]. IEEE Transactions on Smart Grid, 2021, 12(3): 2554-2565.

[13] Han M L, Kwak B I, Kim H K. Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2941-2956.

[14] Rahimifard M, Sizkouhi A M M, Selmic R R. Cyberattack detection for a class of nonlinear multiagent systems using set-membership fuzzy filtering[J]. IEEE Systems Journal, 2024, 18(2): 1056-1067.

[15] Du M N, Xie X P, Wang H, et al. Relaxed co-design of attack detection and set-membership estimation for T-S fuzzy systems subject to malicious attacks[J]. IEEE Transactions on Fuzzy Systems, 2024, 32(5): 2663-2676.

[16] Li J T, Wang Z H, Shen Y, et al. Attack detection for cyber-physical systems: A zonotopic approach[J]. IEEE Transactions on Automatic Control, 2023, 68(11): 6828-6835.

[17] Du M N, Xie X P, Wang H, et al. Relaxed set-membership estimation and cyber attack detection for LPV systems under multiple attacks via a switching-type scheme design[J]. IEEE Transactions on Instrumentation and Measurement, 2024, 73: 3001213.

[18] Uribe-Murcia K J, Shmaliy Y S. Robust UFIR observer for WSNs with multistep random delays and multiple packet dropouts[J]. IEEE Transactions on Automatic Control, 2023, 68(10): 6338-6344.

[19] Xue W, Luan X L, Zhao S Y, et al. A fusion Kalman filter and UFIR estimator using the influence function method[J]. IEEE/CAA Journal of Automatica Sinica, 2022, 9(4): 709-718.

[20] Liu Z, Zhang M, Song X M, et al. A novel fusion maximum correntropy Kalman/UFIR filter for state estimation with uncertain non-Gaussian noise statistics[J]. Measurement, 2023, 220: 113339.

[21] Bhattacharjee D, Subbarao K. Set-membership filter for discrete-time nonlinear systems using state-dependent coefficient parameterization[J]. IEEE Transactions on Automatic Control, 2022, 67(2): 894-901.

[22] Kurzhanskiy A A, Varaiya P. Ellipsoidal toolbox (ET)[C]. Proceedings of the 45th IEEE Conference on Decision and Control. San Diego, 2006: 1498-1503.

[23] Xia N, Yang F W, Han Q L. Distributed networked set-membership filtering with ellipsoidal state estimations[J]. Information Sciences, 2018, 432: 52-62.

[24] Zhai Z Y, Lai G B, Cheng B, et al. Lightweight secure detection service for malicious attacks in WSN with timestamp-based MAC[J]. IEEE Transactions on Network and Service Management, 2022, 19(4): 5299-5311.

[25] He J C, Wang G, Yu H J, et al. Generalized minimum error entropy Kalman filter for non-Gaussian noise[J]. ISA Transactions, 2023, 136: 663-675.

[26] Liu H, Li Y Z, Han Q L, et al. Watermark-based proactive defense strategy design for cyber-physical systems with unknown-but-bounded noises[J]. IEEE Transactions on Automatic Control, 2023, 68(6): 3300-3315.

作者简介

符莎 (1991−), 女, 博士生, 主要研究方向为攻击检测与控制, E-mail: mxshf2009@163.com;

李平 (1964−), 男, 教授, 博士, 博士生导师, 主要研究方向为模型预测控制、自适应控制、工业过程的先进控制和优化, E-mail: lping@ustl.edu.cn;

赵民新 (1987−), 男, 博士生, 主要研究方向为故障检测与容错控制, E-mail: s273337929@foxmail.com.