课程作业-理论引导

理论问题 1——控制系统中的攻击

考虑虚假数据注入 (False data injection, FDI) 攻击下的离散时间 (DT) 系统，其描述为以下状态空间形式：

$$\begin{aligned} x[k+1] &= Ax[k] + Bu[k] + B_a a[k] \\ y[k] &= Cx[k] + D_a a[k] \end{aligned} \tag{1}$$

除题中另有说明外，设 $u[k] = 0$，A 是已知的常数矩阵，$A\ B\ C$ 矩阵如下所示：

$$A = \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 \end{bmatrix}$$

1. 假设攻击者能对 “传感器 1” 和 “执行器 2” 执行虚假数据注入 (FDI) 攻击 $\Delta y_1, \Delta u_2$，请你建模攻击向量 $a[k]$，并完成 B_a 和 D_a 矩阵的设计，以实现上述两种情况下的 FDI 攻击。

2. 回想输出函数 $y[k] = \Phi(x_0, a, k)$ 和无法被检测攻击 (Undetectable Attacks) 的定义。请证明或反驳：“使用 “执行器 2” 的系统(1)存在无法被检测到的攻击” 这一陈述。

Review: $y[k] = \Phi(x_0, a, k) \triangleq CA^k x_0 + C\sum_{i=1}^{k-1} A^{k-i-1} B_a a[i] + D_a a[k]$

3. 假设攻击者只能破坏 “传感器 1”（即所有传感器都可能被破坏），产生无法被检测的攻击 $a[k]$（即在所有 $k \geq 0$ 的时间内产生无法被检测到的非零动态攻击信号）的策略是什么？参数 a_{11}, a_{12}, a_{22} 是如何决定最终系统受到的攻击影响?

Hint: 可对系统(1)构造 *Rosenbrock system matrix* 进行分析。

理论问题 2——传感器攻击下的状态估计

考虑带有多个传感器的离散时间系统，其状态空间表达如(2)所示：

$$\begin{aligned} x[k+1] &= Ax[k] + Bu[k] \\ y_i[k] &= C_i x[k] + a_i[k] \qquad i \in \{1, 2, ..., N\} \end{aligned} \tag{2}$$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

其中 $a_{11} \neq 0, a_{12} \neq 0, a_{22} \neq 0$，你将通过考虑构造不同的矩阵 C_i 和传感器数量 N 来完成以下任务。

1. 假设系统(2)有 $N = 1$ 个输出，$C_i = \begin{pmatrix} 1 & 1 \end{pmatrix}$。当 a_{11}, a_{12}, a_{22} 取何值时系统(2)是可观的?

2. 假设 “传感器 1” 受到攻击，即当 $k \geq 0$ 时 $a_1[k] \neq 0$。系统(2)的状态还能被观测和估计吗？如果可以估计，应该怎么做?

Hint: 建议使用现代控制理论中的 *Luenberger Observer*，推导中遇到困难不妨添加冗余传感器。

3. 常见的状态观测器还有哪些?

理论问题 1——解题思路

1. 根据 $a[k]$ 定义，可得 $a[k] = [\Delta u_2[k], \Delta y_1[k]]^\top$；将 B 划分为 $B = [b_1 b_2]$，得到 B_a 的关系：

$$B_a = b_2 \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

由于 Δy_1 直接添加到测量中，得 $D_a a[k] = \Delta y_1[k]$；由这个关系式和 $a[k]$ 的定义，得到 $Da = [0 \quad 1]$。

2. 由于系统只有一个输出，攻击者可以直接破坏这个信号，因此考虑之前的场景，代入 B_a, D_a：

$$\Phi(x_0, a, k) = CA^k x_0 + C\sum_{i=1}^{k-1} A^{k-i-1} b_2 \Delta u_2[k] + \Delta y_1[k]$$

验证 “执行器 2” 的不可检测攻击的存在性相当于验证以下条件：

(1) $\Phi(x_0, a, k) = 0$ 对某个 x_0^a 成立；

(2) 存在非零的 $\Delta u_2[k]$。

注意: 通过选择传感器损坏，可以满足不可检测条件：$\Delta y_1[k] = -CA^k x_0^a - C\sum_{i=1}^{k-1} A^{k-i-1} b_2 \Delta u_2[k]$，这意味着可以选择任意的 x_0^a 和非零的 $\Delta u_2[k]$，并且通过构建 $\Delta y_1[k]$ 使攻击无法被检测到。

3. 如果 “传感器 1” 被攻击，那么系统可建模为：$a[k] = \Delta y_1[k], B_a = [0 \quad 0]^\top, D_a = 1$。

构造相应的 *Rosenbrock* 矩阵，得到

$$P(z) = \begin{bmatrix} zI - A & -B_a \\ C & D_a \end{bmatrix} = \begin{bmatrix} z - a_{11} & -a_{12} & 0 \\ 0 & z - a_{22} & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

若攻击 $a[k] = z_0^k g$ 不可测，则存在 x_0 满足：

$$P(z_0) \begin{bmatrix} x_0 \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \quad x_0 = \begin{bmatrix} x_{10} \\ x_{20} \end{bmatrix}$$

即：

$$\begin{gathered} (z_0 - a_{11})x_{10} - a_{12}x_{20} = 0 \\ (z_0 - a_{22})x_{20} = 0 \\ x_{10} + g = 0 \end{gathered}$$

其中 $x_{10}, x_{20} \in x_0$，计算 z_0: $detP(z_0) = (z_0 - a_{11})(z_0 - a_{22}) = 0$

因此，要产生不可测的攻击，可以使用的策略有以下两种：

$$\begin{cases} a[k] = z_0^k g = a_{11}^k g \\ g = -x_{10} \\ x_{20} = 0 \\ x_{10} \in \mathbb{C} \end{cases}$$

$$\begin{cases} a[k] = z_0^k g = a_{22}^k g \\ (a_{22} - a_{11})x_{10} - a_{12}x_{20} = 0 \\ g = -x_{10} \end{cases}$$

理论问题 2——解题思路

1. $\begin{pmatrix} C \\ CA \end{pmatrix}$ 满秩。

对于本题的系统，有：

$$rank\begin{pmatrix} C \\ CA \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ a_{11} & a_{12}+a_{22} \end{bmatrix} = n$$

要使以上矩阵满秩，则需满足：$a_{11} \neq a_{12} + a_{22}$

2. 对“传感器 1”建立 *Luenberger observer*:

$$\begin{aligned} \hat{x}[k+1] &= A\hat{x}[k] + Bu[k] + L_1(y_1[k] - \hat{y_1}[k]) \\ &= A\hat{x}[k] + Bu[k] + L_1(y_1[k] - C_1\hat{x}[k]) \\ &= (A - L_1C_1)\hat{x}[k] + Bu[k] + L_1y_1[k] \end{aligned}$$

设观测器估计误差为 $e[k] = x[k] - \hat{x}[k]$，则有：

$$\begin{aligned} e[k+1] &= x[k+1] - \hat{x}[k+1] \\ &= Ax[k] + Bu[k] - (A - L_1C_1)\hat{x}[k] - Bu[k] - L_1y_1[k] \\ &= Ax[k] - (A - L_1C_1)\hat{x}[k] - L_1y_1[k] \end{aligned}$$

带入 $y_1[k] = C_1x[k] - a_1[k]$，整理得：

$$\begin{aligned} e[k+1] &= (A - L_1C_1)x[k] - (A - L_1C_1)\hat{x}[k] - L_1a_1[k] \\ &= (A - L_1C_1)e[k] - L_1a_1[k] \end{aligned}$$

若要观测系统状态，则需要满足 $k \to \infty$ 时，$e \to \infty$，但由于当 $e[k] \to \infty$ 时，$e[k+1] \to -L_1a_1[k]$，而在 $a_1[k]$ 的构造中通常选择不变零点大于 0（即有 $k \to \infty, a_1[k] \to \infty$），因此很难满足 $e[k+1] \to 0$。所以此时无法对系统(2)的状态进行观测和估计。

增加未被攻击的传感“传感器”，并对其建立 *Luenberger observer*：

$$\hat{x}[k+1] = (A - L_2C_2)\hat{x}[k] + Bu[k] + L_2y_2[k]$$

代入 $y_2[k] = C_2x[k]$，则估计误差为：

$$\begin{aligned} e[k+1] &= Ax[k] + Bu[k] - (A - L_2C_2)\hat{x}[k] - Bu[k] - L_2y_2[k] \\ &= (A - L_2C_2)(x[k] - \hat{x}[k]) \\ &= (A - L_2C_2)e[k] \end{aligned}$$

此时要满足 $k \to \infty$ 时，$e[k] \to 0$，只需选择合适的 L_2 使 $A - L_2C_2$ 的所有特征值均具有负实部即可（e 稳定衰减）。如果存在这样的 L_2（对“传感器 2”而言，系统是可观的）则系统(2)的真实状态可被观测；如果不存在，则可以继续增加传感器。

3. 可考虑 *Kalman Filter* 及其变种。