事件触发抵御DoS攻击

#控制理论与实践

讨论多智能体系统中，使用事件触发机制抵御网络攻击的一种方案

参考文献：

Z. Feng and G. Hu, "Secure Cooperative Event-Triggered Control of Linear Multiagent Systems Under DoS Attacks," in *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 741-752, May 2020, doi: 10.1109/TCST. 2019.2892032.

1. 问题形式

1.1 多智能体网络模型

动力学方程使用如下形式的表述：

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad t \in \mathbb{R}_{\geq 0}$$

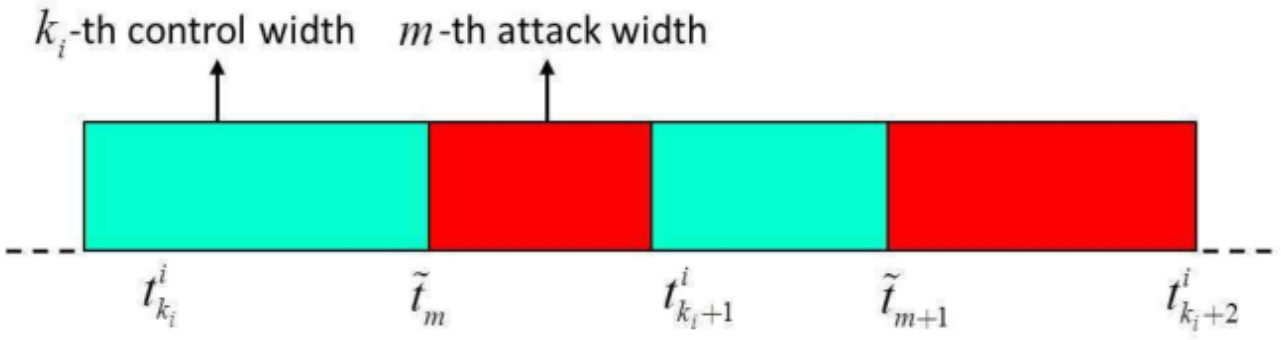
在这篇文章中，A 不必是 Hurwitz 矩阵
（注：Hurwitz 矩阵要求所有特征值的实部均为负数，此时系统可以是渐近稳定的。）

分布式控制器定义如下：

$$u_i(t) = K\zeta_i(t), \quad \zeta_i(t) = \sum_{j=1}^{N} a_{ij}(x_j(t) - x_i(t))$$

其中，$\zeta_i(t)$ 是一致性误差。

1.2 DoS 攻击模型



DoS 攻击可以同时作用于测量通道和控制通道。
攻击序列如上图所表示。
攻击指示序列：$\{\tilde{t}_m\}_{m\in\mathbb{N}}$，最小攻击时长 $\tilde{\Delta}_m > 0$，DoS 攻击时段为：$\mathcal{A}_m = [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m)$
在一段时间内的拒绝服务时长可以表示为 ：

$$\Xi_a(\tau, t) = \cup\mathcal{A}_m \cap [\tau, t], \quad m \in \mathbb{N}$$

在此区间内的允许通信时间为：

$$\Xi_s(\tau, t) = [\tau, t] \setminus \Xi_a(\tau, t).$$

1.2 控制目标

无领导者的控制目标：

$$\|x_i(t) - x_j(t)\|^2 \le \kappa e^{-\rho(t-t_0)}, \quad \forall t > t_0.$$

存在领导者的控制目标：

$$\|x_i(t) - x_0(t)\|^2 \le \tilde{\kappa} e^{-\tilde{\rho}(t-t_0)} \|x_i(t_0) - x_0(t_0)\|^2.$$

2 DoS 攻击下的无领导者一致性

2.1 事件触发控制器设计

$t_0 = t_0^i, t_1^i, \ldots, t_{k_i}^i, \ldots$ 是事件触发时刻，在任意两个时刻之间，控制信号被定义设计为：

$$u_i(t) = K\hat{\xi}_i(t), \quad \hat{\xi}_i(t) = \sum_{j \in \mathcal{N}_i(\mathcal{G})} a_{ij}(\hat{x}_j(t) - \hat{x}_i(t))$$

$\hat{x}_i(t) = x_i(t_{k_i(t)}^i)$ 是最近一次的采样状态，本文的新颖之处在于一致性误差的估计值仅依赖于智能体状态的估计值。

$$k_i(t) = \begin{cases} -1, & \text{if } \Xi_s(0,t) = \emptyset, \\ \sup\{k_i \in \mathbb{N} | t_{k_i}^i \in \Xi_s(0,t)\}, & \text{otherwise} \end{cases}$$

定义一些初始值：$k_i(0) = -1$ ，如果刚开始就被攻击，则初始控制为 0，-1 时刻的一致性误差估计值为 0。
（注：-1 时刻的一致性误差值定义只是为了方便推导。）
邻居的状态是单独更新的，同样也是在事件触发时刻进行更新，使用如下的更新方案：

$$\dot{\hat{x}}_j(t) = A\hat{x}_j(t), \quad t_{k_j}^j \leq t < t_{k_j+1}^j \hat{x}_j(t_{k_j}^j) = x_j(t_{k_j}^j), \quad j \in \mathcal{N}_i(\mathcal{G}), \quad k_j \in \mathbb{N}$$

对状态的补充说明：对一个智能体，其自身和其邻居在事件触发时间间隔内，都会按照上面的方程进行自更新，一旦出现了事件触发时刻，就会进行采样获取真实值。
每个智能体都需要获取一致性误差以用于更新，为了确定触发时刻，定义一个测量误差：$e_i(t) = \hat{x}_i(t) - x_i(t).$
期望一种事件触发：$\|e_i(t)\| \leq \beta_i \|\hat{\xi}_i(t)\|, \quad 0 < \beta_i < 1, \quad i = 1, \ldots, N$
（注：被攻击时控制器置 0，且无法重置测量误差）
（注：系统可以自己确定事件触发条件，由于使用了基于模型的估计，即使 A 不稳定，智能体也能预测自己的失控趋势。）
为确保不出现 Zeno 行为，使用如下的方法来确定事件触发时间：

$$t_{k_i+1}^i = \begin{cases} t_{k_i}^i + \vartheta_i, & \text{if } k_i \in \mathcal{F} \\ t_{k_i}^i + \Delta_{k_i}^i, & \text{otherwise} \end{cases}$$

（注：在 DoS 攻击期间，为避免频繁触发强制使用一个正常数作为间隔；在正常通信期间，选取自然事件触发间隔和保底时间中的最大值，强制避免 Zeno 行为。）

$$\mathcal{F} := \{(i, k_i) \in \mathcal{V} \times \mathbb{N} \mid t^i_{k_i} \in \cup_{m\in\mathbb{N}} \mathcal{A}_m\}$$

$$t^i_{k_i} = \inf_{t>t^i_{k_i}} \{t - t^i_{k_i} \mid \|e_i(t)\| = \beta_i \|\hat{\xi}_i(t)\|\}.$$

2.2 DoS 攻击频率和攻击周期

频率：

$$N_a(T_1, T_2)$$

$$F_a(T_1, T_2) = \frac{N_a(T_1, T_2)}{T_2 - T_1}$$

周期刻画，存在一个尺度：

$$T_a(T_1, T_2) \le T_0 + \frac{T_2 - T_1}{\tau_a}.$$

用于表征攻击一定存在，且攻击时长有界。

2.3 无领导者下一致性共识的稳定性分析

假设：图是连通的。

$$e(t) = \mathrm{col}(e_1(t), \ldots, e_N(t)), x(t) = \mathrm{col}(x_1(t), \ldots, x_N(t)), \text{ and } \hat{x}(t) = \mathrm{col}(\hat{x}_1(t), \ldots, \hat{x}_l$$

$$\dot{\hat{x}}(t) = [I_N \otimes A - (\mathcal{L} \otimes BK)]x(t) - (\mathcal{L} \otimes BK)e(t).$$

对智能体的平均状态进行定义：$\bar{x}(t) = \frac{1}{N}\sum_{i=1}^{N} x_i(t) = \frac{1}{N} 1_N^T x(t).$
同时定义不一致向量：$\delta_i(t) = x_i(t) - \bar{x}(t)$
$\delta(t) = (I_N - \frac{1}{N} 1_N 1_N^T)x(t) = (\mathcal{M} \otimes I_n)x(t).$
（注：上式通过简单的维度扩展思考即可得到。）
接下来讨论一下线性变换
$\mathcal{L}$ 是对称半正定矩阵。
由 $\delta(t)$ 的定义很容易可以看出，$(1_N^T \otimes I_n)\delta(t) = 0.$
因而，总是存在一个正交矩阵：$\Psi = \left[\frac{1_N}{\sqrt{N}}, \Phi\right] \in \mathbb{R}^{N\times N}$
其中的 Φ 是 $\mathcal{L}$ 中正交向量对对应的特征值。
（注：根据（针对对称矩阵），它可以被正交对角化）

（谱定理：任何 $N\times N$ 对称矩阵 L，都存在一组**正交单位特征向量**，构成一个正交矩阵 Ψ，使得 $\Psi^T L\Psi$ 是对角矩阵（对角元为 L 的特征值）

（注：单位特征向量+正交单位特征向量）

$$\Psi^T\Psi = I_N,\quad \Phi\Phi^T = \mathcal{M} = I_N - \frac{1_N 1_N^T}{N}, \mathcal{L}\mathcal{M} = \mathcal{M}\mathcal{L} = \mathcal{L},\quad \Psi^T\mathcal{L}\Psi = \mathrm{diag}[0, \lambda_i(\mathcal{L})].$$

（注：拉普拉斯矩阵是半正定的，且有一个特征值为 0，对应的特征向量全 1，所有特征值非负，若图是连通的，则只有一个 0 特征值）

（注：$\Phi\Phi^T$ 列向量与 1_N 正交，即投影到不一致向量所在的子空间）

（注：$\mathcal{L}\mathcal{M} = \mathcal{M}\mathcal{L} = \mathcal{L}$ 表示了矩阵投影到子空间）

（注：矩阵投影具有幂等性，分解性，对称性）

（注：$\Psi^T\mathcal{L}\Psi = \mathrm{diag}[0, \lambda_i(\mathcal{L})]$ 表征了对称矩阵对角化的结果）

不一致向量的动力学方程：

$$\dot{\delta}(t) = [I_N \otimes A - (\mathcal{L}\otimes BK)]\delta(t) - (\mathcal{L}\otimes BK)e(t).$$

为了在后续稳定性分析中清晰表达，定义 $\mathfrak{B} = \frac{1}{c_1}\ln\left(\frac{c_1}{c_2}\sqrt{c}+1\right)$，其中 $c = 2\gamma_2\lambda_N^2(\mathcal{L})/(N(1-s_{\max}))$，

$\gamma_2 > 0,\quad s_{\max} = \max_{i\in\mathcal{V}} s_i < \frac{\lambda_{\min}^2(Q)}{4k_0^2\lambda_N^2(\mathcal{L})+\lambda_{\min}^2(Q)}$，$k_0 = \|PBK\|$，

$c_1 = 2\|A\| + c_2,\quad c_2 = \lambda_N(\mathcal{L})\|BK\|(1+\sqrt{N}c)$，$P$ 是 ARE 方程中待求解的矩阵。

A）无领导者无网络攻击稳定性证明

考虑采样时间间隔后，定义了一个新的 DoS 攻击区间

$\mathfrak{A}_m = [\tilde{t}_m, \tilde{t}_m + \tilde{\Delta}_m + \Delta_*).$

从而定义新的区间：

$$\widetilde{\Xi}_a(\tau,t) := \cup\mathfrak{A}_m \cap [\tau,t],\quad \widetilde{\Xi}_s(\tau,t) := [\tau,t]\setminus\Xi_a(\tau,t).$$

正常通信区间内，构建如下的利李雅普诺夫函数：

$$V(t) = \delta^T(t)(I_N\otimes P)\delta(t)$$

$$\dot{V}(t) = \delta^T\left(I_N\otimes(PA+A^TP)\right)\delta - 2\delta^T(\mathcal{L}\otimes PBK)(\delta+e)$$

定义：$\tilde{\delta} = (\Psi^T\otimes I_n)\delta$，$\tilde{\delta}_1 = ((1_N^T/N)\mathcal{M}\otimes I_n)x = 0$，$\tau \geq (2\lambda_2(\mathcal{L}))^{-1}$

（注：$K = \tau K_0$）

（注：1．将误差分解为一致性分量和非一致性分量 2．最严格的负定条件来自于 λ_2，分母越大，负定程度越高）
（注：λ_2 最小意味着 $\dot{V}_2=\tilde{\delta}_2^T(PA+A^TP-2\lambda_2PBK)\tilde{\delta}_2$ 最难满足负定）
(注：$\tilde{\delta}$ 变换是为了对拉普拉斯矩阵进行正交化，从而引出特征值，然后使得第二最小特征值满足矩阵块负定)
（注：负定的求解过程，将不等式转化为标量条件，再利用范数性质求解）
综上，得：

$$\delta^T[I_N\otimes(PA+A^TP)-2\tau(\mathcal{L}\otimes PBR^{-1}B^TP)]\delta\leq\sum_{i=2}^{N}\tilde{\delta}_i^T(PA+A^TP-PBR^{-1}B^TP)$$

利用杨不等式变换，得：

$$-2\delta^T(\mathcal{L}\otimes PBR^{-1}B^TP)e\leq k_0\sum_{i=2}^{N}(\omega\tilde{\delta}_i^T\tilde{\delta}_i+q^{-1}\tilde{e}_i^T\tilde{e}_i)$$

其中：$k_0=||PBK||,\omega=\lambda_N^2((L)),\tilde{e}=(\Phi^T\otimes I_n)e$
（注：双线性项的放缩

令 $a=\delta^\top(\sqrt{\mathcal{L}\otimes X}),\ b=\sqrt{\mathcal{L}\otimes X}e,$ 则: $-2\delta^\top(\mathcal{L}\otimes X)e\leq\omega\delta^\top(\mathcal{L}\otimes X)\delta+q^{-1}e^\top(\mathcal{L}$

，再利用拉普拉斯特征值上界

$$\mathcal{L}=\Psi\Lambda\Psi^\top,\ \text{误差}\ \tilde{\delta}=(\Psi^\top\otimes I_n)\delta,\ \tilde{e}=(\Psi^\top\otimes I_n)e,$$

得：

$$\delta^\top(\mathcal{L}\otimes X)\delta=\sum_{i=2}^{N}\lambda_i^2\tilde{\delta}_i^\top X\tilde{\delta}_i\leq\omega\sum_{i=2}^{N}\tilde{\delta}_i^\top X\tilde{\delta}_i,e^\top(\mathcal{L}\otimes X)e=\sum_{i=2}^{N}\lambda_i^2\tilde{e}_i^\top X\tilde{e}_i\leq\omega\sum_{i=2}^{N}\tilde{e}_i^\top X$$

（注：根据瑞丽商定理，得到 $\delta_i^TQ\delta_i\geq\lambda_{\min}(Q)\|\delta_i\|^2$，）

其中 $\|\tilde{e}\|\leq\|\Phi^T\otimes I_n\|\|e\|\leq\|e\|$
利用了 $\|\Phi^T\otimes I_n\|=1$
令 $\hat{\xi}(t)=\mathrm{col}(\hat{\xi}_1,\ldots,\hat{\xi}_N)=\sum_{j\in\mathcal{N}_i(G)}a_{ij}(\hat{x}_j(t)-\hat{x}_i(t))$
$e_i(t)=\hat{x}_i(t)-x_i(t)$

$$\|\hat{\xi}(t)\|=\|-(\mathcal{L}\otimes I_n)(x+e)\|=\|\xi-(\mathcal{L}\otimes I_n)e\|\leq\|\xi\|+\|(\mathcal{L}\otimes I_n)e\|\leq\|\xi\|+\lambda_N(\mathcal{L}$$

其中：$\xi_i(t)=\sum_{j\in\mathcal{N}_i(\mathcal{G})}a_{ij}(x_j(t)-x_i(t))$，由于 $\mathcal{L}^2\le\lambda_N^2(\mathcal{L})\mathcal{M}^2$
得：

$$\|\xi\|^2=x^T(\mathcal{L}^T\otimes I_n)(\mathcal{L}\otimes I_n)x=x^T(\mathcal{L}^2\otimes I_n)x\le\lambda_N^2(\mathcal{L})x^T(\mathcal{M}^2\otimes I_n)x=\lambda_N^2(\mathcal{L})\|\delta\|^2$$

得到：$\|\hat{\xi}(t)\|\le\lambda_N(\mathcal{L})(\|\delta\|+\|e\|)$，
由于 $\|e_i(t)\|\le\beta_i\|\hat{\xi}_i\|$，$\beta_i^2=\frac{s_i}{(2\lambda_N^2(\mathcal{L}))}$
定义 $s_{max}=max_i s_i$ ，$\|e_i(t)\|\le s_{\max}\|\hat{\xi}\|^2/(2\lambda_N^2(\mathcal{L}))\le s_{\max}(\|\delta\|^2+\|e\|^2)$
导致了：$\|e(t)\|^2\le s_{\max}\|\delta\|^2/(1-s_{\max})$
（注：s 是误差上界系数）
通过选择 s_{max} 和 α ,得：

$$\dot{V}(t)\le-\left(\frac{\lambda_{\min}(Q)}{2}-\frac{2k_0^2\lambda_N^2(\mathcal{L})s_{\max}}{\lambda_{\min}(Q)(1-s_{\max})}\right)\sum_{i=1}^{N}\delta_i^T\delta_i\le-\alpha_1\delta^T(t)(I_N\otimes P)\delta(t)=-\alpha$$

A）无领导者有网络攻击稳定性证明