中国科学 : 信息科学 2026 年 第 56 卷 第 5 期: 1089–1100
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
安全控制理论与应用专题 • 论文

DoS 攻击下具有状态约束的非线性系统网络安全控制

宋若琳[1], 洪奕光[1,2], 董怡[1,2*], 辛斌[3], 王晴[3], 陈曦[4]

1. 同济大学自主智能无人系统科学中心, 上海 201210
2. 同济大学电子与信息工程学院, 自主智能无人系统全国重点实验室, 上海 201804
3. 北京理工大学自动化学院, 北京 100081
4. 香港中文大学机械与自动化工程系, 香港 999077
* 通信作者. E-mail: yidong@tongji.edu.cn

收稿日期: 2025–11–05; 修回日期: 2026–02–12; 接受日期: 2026–03–16; 网络出版日期: 2026–04–16

国家自然科学基金 (批准号: 62473287, 62088101) 和上海市科技重大专项 (批准号: 2021SHZDZX0100) 资助项目

摘要 针对状态受约束且遭受随机拒绝服务 (denial of service, DoS) 攻击的非线性系统, 本文研究其网络安全镇定控制问题. 提出了一种融合时间与事件触发的混合采样机制, 进而基于障碍函数设计了一类双重安全控制器. 该控制方法能够在严格维持系统状态不违背预设约束的前提下, 有效节约通信资源, 并具备对 DoS 攻击的良好容错性能. 理论分析表明, 闭环控制系统可实现半全局渐近稳定, 进一步验证了所提控制律在稳定性与鲁棒性方面的理论可行性. 数值仿真结果表明, 在一定的攻击频率与持续时间范围内, 本文方法能够快速抑制外部扰动, 驱动系统状态收敛至平衡点, 从而显著增强系统在 DoS 攻击环境下的抗干扰能力与运行可靠性.

关键词 DoS 攻击, 非线性控制, 状态约束, 障碍函数, 混合触发

1 引言

在实际的网络化控制系统中, 由于其开放性和不确定性, 通信网络容易遭受拒绝服务 (denial of service, DoS) 攻击的威胁 [1]. 此类攻击通过消耗网络资源, 阻断数据传输路径, 严重削弱了控制系统的稳定性和可靠性, 甚至在极端情况下可能导致系统失控 [2]. 因此, 研究在 DoS 攻击环境下如何解决非线性系统的网络安全控制问题, 具有重要的理论意义和工程实践意义. 同时, 许多实际应用系统, 如飞行器 [3]、无人车 [4] 以及各类工业控制过程 [5], 通常伴随有严格的状态约束条件. 如果控制策略无法保证系统状态始终处于设定的安全范围内, 就可能产生设备损坏甚至人身伤害的风险. 因此, 对 DoS 攻击下非线性系统的安全约束控制问题的研究, 既具有重要的学术价值, 也具有十分迫切的现实应用需求.

近年来, 针对拒绝服务攻击下系统稳定性与网络安全控制策略的研究正在不断深入. DoS 攻击通过干扰信息交互的时间, 影响了网络化控制系统的安全性. 首先研究目前较为常用的 DoS 攻击模型, 并通过设定攻击频率和持续时间的假设条件, 建立了线性系统的闭环稳定性判据 [6]. 同时多传输信道下 DoS 攻击的输入到状态稳定性问题也得到了进一步的研究 [7]. 在多智能体系统领域, Feng 等 [8] 提出了基于事件触发更新规则的安全一

引用格式: 宋若琳, 洪奕光, 董怡, 等. DoS 攻击下具有状态约束的非线性系统网络安全控制. 中国科学: 信息科学, 2026, 56: 1089–1100, doi: 10.1360/SSI-2025-0478
Song R L, Hong Y G, Dong Y, et al. Secure control of nonlinear systems under DoS attacks with state constraints. Sci Sin Inform, 2026, 56: 1089–1100, doi: 10.1360/SSI-2025-0478

致性协同控制策略, 而针对领航者 – 跟随者的一致性问题, 一种基于事件触发的控制方法证明了该问题的可解性 [9]. 针对 DoS 攻击下的离散异构多智能体系统, 一种基于弹性观测器的数据驱动控制方法实现了在有向网络中的输出一致性 [10]. 现有 DoS 攻击下的安全控制方法主要针对线性系统, 非线性系统研究仍然相对有限. 例如, Wang 等 [11] 针对 DoS 攻击下的领导者 – 跟随者多智能体系统, 提出了一种基于观测器的分布式事件触发控制策略, 以实现网络安全一致性控制; 针对一类非线性多智能体系统在 DoS 攻击下的弹性跟踪控制问题, 结合模糊自适应控制及协同观测器的方法确保了系统的稳定性 [12]. 然而, 在面对随机性强或持续时间较长的 DoS 攻击时, 单一触发机制的控制精度与稳定性仍难以保证, 不确定非线性系统的性能容易退化甚至失稳.

另一方面, 受限控制系统是控制理论中的一个重要研究领域, 其根本挑战在于如何设计控制器, 使系统变量在整个运行期间满足预设的硬约束. 针对非线性纯反馈系统, 一种基于障碍李雅普诺夫函数的反步自适应控制器, 有效处理了全状态约束问题 [13]; 此外一种基于统一障碍函数的鲁棒自适应控制方法, 能够在无需依赖可行性条件的前提下, 处理具有动态与非对称特性的状态约束 [14]; 针对全状态受限的欧拉 – 拉格朗日系统, 结合误差变换与障碍李雅普诺夫函数的预设性能控制方法, 实现了跟踪误差在有限时间内收敛至预设区间, 并最终渐近趋于零的控制目标 [15]; Geng 等 [16] 则通过构造新型障碍函数, 将有约束与无约束情形纳入统一分析框架, 结合滑模控制与神经网络技术, 设计了一类自适应固定时间控制器, 进一步拓展了状态约束控制的理论方法与应用范围.

然而, 现有基于状态约束的研究大多建立在理想的通信条件下, 对于随机 DoS 攻击环境下状态约束问题的系统性分析相对匮乏. 针对 DoS 攻击下的非线性多智能体系统, 一种安全编队控制方法, 利用模糊方法处理系统不确定性, 并结合障碍李雅普诺夫函数实现了输出约束 [17] . 总体而言, DoS 攻击下的安全控制与状态约束控制虽已分别取得一定成果, 但其研究路径多为各自独立开展, 前者注重在攻击环境下的稳定性与通信容错, 却较少关注状态约束的严格保持; 后者强调维持系统在受限情况下的运行, 却往往忽视网络攻击引发的通信中断问题. 因此, 在 DoS 攻击环境下实现系统的低通信开销、状态约束安全与闭环稳定性的统一, 仍然是急需解决的重要科学问题.

本文研究了一类 DoS 攻击下状态受限的不确定非线性系统的网络安全控制问题, 目标是在通信受扰条件下同时保障状态安全, 缓解 DoS 攻击影响并稳定闭环系统. 基于这一目标, 本文的贡献体现在两个方面. 首先, 针对现有基于控制障碍函数的安全控制通常依赖连续状态, 而 DoS 攻击会造成控制的间歇更新从而难以兼顾稳定性与安全性的问题, 本文在障碍函数框架内引入明确的有界标志值, 用于判定状态是否逼近安全边界, 并在进入边界邻域时利用控制机制增强约束, 同时与混合采样机制结合, 直接采用采样状态进行反馈控制, 从而摆脱对连续状态监测的依赖, 使系统在 DoS 导致更新受限时仍能保持状态始终满足安全约束. 其次, 针对系统在 DoS 攻击窗口内呈现开环运行特征, 本文采用高增益控制抑制未知非线性项的增长, 并在无 DoS 区间构造足够强的指数收敛速率以抵消 DoS 区间内的开环增长上界, 在此基础上, 进一步建立控制参数与 DoS 攻击频率及持续时间之间的关系, 从理论上保证闭环轨迹在不确定攻击下仍保持状态受限并实现渐近镇定.

本文的后续安排如下: 第 2 节构建拒绝服务攻击模型与非线性系统模型, 并给出问题的数学描述; 第 3 节详述障碍函数、混合采样机制与控制器的设计过程; 第 4 节进行系统的稳定性分析, 给出并证明主要定理; 第 5 节通过仿真验证所提控制方法的有效性与优越性; 最后, 第 6 节总结全文并展望未来研究方向.

2　问题描述

首先, 考虑一个非线性不确定仿射系统, 定义为

$$\dot{x} = g\left(x, w\right) + b\left(w\right) u, \tag{1}$$

其中, $x(t) \in \mathbb{R}^n$ 为状态量, $u(t) \in \mathbb{R}^n$ 为控制输入, $w \in W \subset \mathbb{R}^{n_w}$ 为不确定参数, 且 W 为 $\mathbb{R}^{n_w}$ 中包含原点的紧子集. 系统的状态始终满足约束 $\|x(t)\| \leqslant k_c$, 其中 k_c 为一个正的常数. 函数 $g(\cdot)$ 为连续可微函数, 且满足对于所有 $w \in W$, 都有 $g(0, w) = 0$. $b(w) \in \mathbb{R}$ 为一个标量函数, 表示控制系数, 且 $b(w) > 0$. 如果对任意 $\forall t \geqslant 0$, 有

$x(t) \in S$, 则称系统满足约束, 其中

$$\begin{aligned} S &= \{x \in \mathbb{R}^n : \|x\| < k_c\}, \\ \partial S &= \{x \in \mathbb{R}^n : \|x\| = k_c\}. \end{aligned} \tag{2}$$

假设 $\bar{S} = S \cup \partial S$ 是一个非空的连通集. 定义可行域集合 S_s 及初始安全集合 S_I,

$$S_s = \{x \in \mathbb{R}^n : \|x\| \leqslant k_c - k_{c0}\}, \tag{3}$$

$$S_I = \{x(0) \in \mathbb{R}^n : \|x(0)\| \leqslant k_c - \bar{k}_{c0}\}, \tag{4}$$

其中, $0 < k_{c0} < \bar{k}_{c0} < k_c$.

考虑非线性系统 (1) 控制器与执行器之间的通信信道遭受非周期性随机拒绝服务攻击. 为有效分析拒绝服务攻击的影响机制, 急需建立精确的数学模型. 用序列 $\{\bar{h}_p\}_{p\in\mathbb{N}^+}$ 来表示 DoS 攻击开关状态转换时刻, 且 $\bar{h}_0 > 0$. 定义第 p 次 DoS 攻击时间区间为 $\bar{H}_p = \{\bar{h}_p\} \cup [\bar{h}_p, \bar{h}_p + \bar{\tau}_p)$, $\bar{\tau}_p \geqslant 0$ 表示信号 $u(t)$ 无法传输的持续时长. 如果 $\bar{\tau}_p = 0$, 则第 p 个 DoS 攻击在时间 $\bar{h}_p$ 时表现为单个脉冲. 当每个时间区间 $[\tau, t]$ 满足 $t \geqslant \tau \geqslant 0$ 时, 定义信号传输被拒绝的时间集合 $\bar{\Xi}(\tau, t)$ 与被允许的时间集合 $\bar{\Theta}(\tau, t)$ 分别为

$$\bar{\Xi}(\tau, t) = \bigcup_{p\in\mathbb{N}} \left(\bar{H}_p \cap (\tau, t)\right), \quad \bar{\Theta}(\tau, t) = (\tau, t) \setminus \bar{\Xi}(\tau, t). \tag{5}$$

令 $n(\tau, t)$ 表示在时间区间 $(\tau, t]$ 内 DoS 开关转换的次数, 提出以下假设条件.

假设1　存在常数 $\xi \in R > 0$ 和 $\tau_D \in R > \tau_m$, 使得

$$n(\tau, t) \leqslant \xi + \frac{t - \tau}{\tau_D}, \tag{6}$$

其中, τ_m 为硬件平台允许的最小采样间隔.

假设2　存在常数 $\kappa \in R \geqslant 0$ 和 $T \in R \geqslant 1$, 满足

$$\left|\bar{\Xi}(\tau, t)\right| \leqslant \kappa + \frac{t - \tau}{T}. \tag{7}$$

注释1　假设 1 与 2 是针对拒绝服务攻击下网络安全控制问题的标准假设, 参考文献 [6,18]. 基于文献 [19] 引入的平均驻留时间概念, 假设 1 用于限制 DoS 攻击频率, 确保连续两次 DoS 触发间的平均间隔大于 τ_m, 最小更新间隔 τ_m 是硬件平台固定属性, 是提前给定的. 在较大时间区间内, 当 $\frac{t-\tau}{\tau_D}$ 相对于 ξ 占主导时, DoS 触发次数至多为 $\frac{t-\tau}{\tau_D}$ 量级, 小于 $\frac{t-\tau}{\tau_m}$. 假设 2 针对 DoS 攻击持续时间, 可保证无信号传输的时间区间不超过某个时间比例. ξ 与 κ 为正则化项, 使不等式 (6) 与 (7) 保持一致.

由于 DoS 攻击的发生具有随机性, 在控制器设计中 $\bar{h}_p$ 与 $\bar{\tau}_p$, $p \in \mathbb{N}^+$ 通常未知. 为检测 DoS 是否发生, 本文利用基于 TCP (transmission control protocol) 的通信机制进行判别, 该机制具备双向传输与确认反馈. 为此, 定义两组非负数序列 $\{h_p\}_{p\in\mathbb{N}^+}$ 与 $\{\tau_p\}_{p\in\mathbb{N}^+}$, 分别用于记录检测到的 DoS 攻击起始时刻及其持续时长. 对采样序列 $\{t_k\}_{k\in\mathbb{N}}$, 若在 $t = t_k$ 时刻控制输入 $u(t)$ 通过控制器 – 执行器通道成功接收并得到确认, 则判定当前通信可用, 即不存在 DoS 攻击, 利用最新采样数据更新控制量. 若在 $t = t_{k+1}$ 时刻, 确认包 (acknowledge character, ACK) 无法按时返回, 系统可通过确认包超时或连续未确认等通信层反馈, 判定在区间 $[t_k, t_{k+1})$ 内发生 DoS 攻击, 用 h_p 记录检测到 DoS 的起始时刻, 并令 $u(t) = 0$, 用 $h_p + \tau_p$ 记录其结束时刻, 将检测到的 h_p 时刻 DoS 发生的区间定义为 $H_p = \{h_p\} \cup [h_p, h_p + \tau_p)$, 其中 $h_0 = 0$, $\tau_0 = 0$. 对应的 h_p 前一时刻不发生 DoS 的区间为 $W_{p-1} = \{h_{p-1} + \tau_{p-1}\} \cup [h_{p-1} + \tau_{p-1}, h_p)$. 在时间区间 $[\tau, t]$, $t \geqslant \tau \geqslant 0$ 内, 记录检测到的 DoS 发生及不发生的时间集合分别为 $\Xi(\tau, t) = \bigcup_{p\in\mathbb{N}^+} H_p \cap [\tau, t]$ 及 $\Theta(\tau, t) = \bigcup_{p\in\mathbb{N}^+} W_{p-1} \cap [\tau, t]$.

本文主要关注 DoS 攻击作用下非线性系统控制器 – 执行器通道信号传输受阻场景. 此时, 考虑 DoS 攻击的执行器端实际输入信号为

$$u(t) = \begin{cases} u_0(t_k), & t \in [h_{p-1} + \tau_{p-1}, h_p), \\ 0, & t \in [h_p, h_p + \tau_p), \end{cases} \tag{8}$$

其中, $u_0(t)$ 为状态受限的非线性控制器.

假设3　存在常数 $b_m > 0$ 和 $b_M > 0$, 使得 $b_m \leqslant b(w) \leqslant b_M$.

注释2　参考文献 [20], 假设 3 为保证控制器设计的可行性提供了必要基础.

因此, 可以将受限的不确定非线性系统 (1) 网络安全镇定控制问题表述如下.

问题1　考虑受拒绝服务影响的不确定系统 (1), 且 DoS 攻击由式 (5) 给出. 对于任意初始状态 $x(0) \in S$, $\forall t \geqslant 0$, 设计一个双重安全控制策略 $u(t)$ 形式如式 (8), 使得闭环系统的轨迹存在, 且满足对所有 $t \geqslant 0$, $x(t) \in S$ 且 $\lim_{t\to\infty} x(t) = 0$.

3　双重安全控制器设计

针对不确定非线性仿射系统 (1), 本节基于障碍函数方法对系统进行坐标变换, 将系统转换为一个无约束系统, 并且设计了一种融合时间触发与事件触发的双重安全控制器. 该控制方法通过在时间触发与事件触发机制之间动态切换, 克服了单一触发方式的局限性, 在实现状态约束的前提下, 提升了系统对攻击的响应速度, 有效降低通信资源消耗. 后续严格证明了闭环系统在 DoS 攻击下的稳定性和安全性.

步骤 1: 障碍函数设计. 定义函数 $\mu(\cdot) : S \to \mathbb{R}$ 为

$$\mu(x) = \frac{1}{k_c^2 - \|x\|^2}. \tag{9}$$

令 $\rho(x) = \frac{2xx^{\mathrm{T}}}{k_c^2 - \|x\|^2} + I_n$. 为了将状态受限的非线性系统转换为一个不受约束的系统, 进行基于障碍函数的坐标变换

$$z = \mu(x)x. \tag{10}$$

则将系统 (1) 转换为

$$\dot{z} = \begin{cases} \mu\rho g(x,w) + \mu\rho b(w)\, u_0(t_k), & t \in [\, h_{p-1} + \tau_{p-1},\, h_p\,), \\ \mu\rho g(x,w), & t \in [\, h_p,\, h_p + \tau_p\,). \end{cases} \tag{11}$$

步骤 2: 状态受限的非线性控制器设计. 由式 (1) 可知, $g(0,w) = 0$, 根据推论 11.1 [21], 存在光滑函数 $\bar{\gamma}(w) \geqslant 0$ 和 $\hat{\gamma}(x) \geqslant 0$, 使得 $||g(x,w)|| \leqslant \bar{\gamma}(w)\hat{\gamma}(x)||x||$. 对于 $w \in W$, 存在正常数 $\tilde{\gamma} \geqslant 0$, 使得 $\bar{\gamma}(w) \leqslant \tilde{\gamma}$. 令 $\gamma(x) = \tilde{\gamma}\hat{\gamma}(x)$, 则有 $||g(x,w)|| \leqslant \gamma(x)||x||$.

结合系统 (11), 可以设计状态受限的非线性控制器为

$$u_0(t) = -\frac{1}{2b_m}(\mu\rho)^{-1}(m_1 + P(x))z(t), \tag{12}$$

其中, $m_1 > 0$, $P(x) \geqslant 1$ 为充分光滑的正函数, 其具体形式将在后文给出. m_1 与状态相关增益 $P(x)$ 用于调节闭环稳定裕度与鲁棒性, 该负反馈有效抑制误差变量 $z(t)$; 同时, $P(x) \geqslant 1$ 使得系统状态接近约束边界时控制作用增强, 从而将轨迹推回安全集合内部. 此外, 在 DoS 时序与混合采样机制下, 采样引入的误差上界可与该增益结构及平均驻留时间条件结合, 便于后续 Lyapunov 分析的分段估计.

步骤 3: 混合采样机制设计. 基于第 2 节中的 DoS 检测机制, 本文提出一种混合采样方法, 将时间触发与事件触发相结合, 并通过 TCP 机制在线检测 DoS 状态实现采样方式切换. 区别于传统采样方式, 本文采用不同采样方式在安全性与通信负载之间实现权衡. 当检测到 DoS 攻击时, 系统切换为基于时间的采样方法, 在通信恢复的可用窗口内以固定频率进行补偿式更新, 以抑制采样误差在攻击段的累积. 当处于无攻击时段, 系统采用基于事件触发的采样方法, 仅当采样误差达到阈值时才更新, 从而在保证稳定与约束均满足的前提下减少不必要的通信与计算.

在时间区间 $t \in [t_k, t_{k+1}), k \in \mathbb{N}$ 上, 定义由采样机制引入的状态受限的非线性控制器误差为

$$u_s(t) = u_0(t_k) - u_0(t), \tag{13}$$

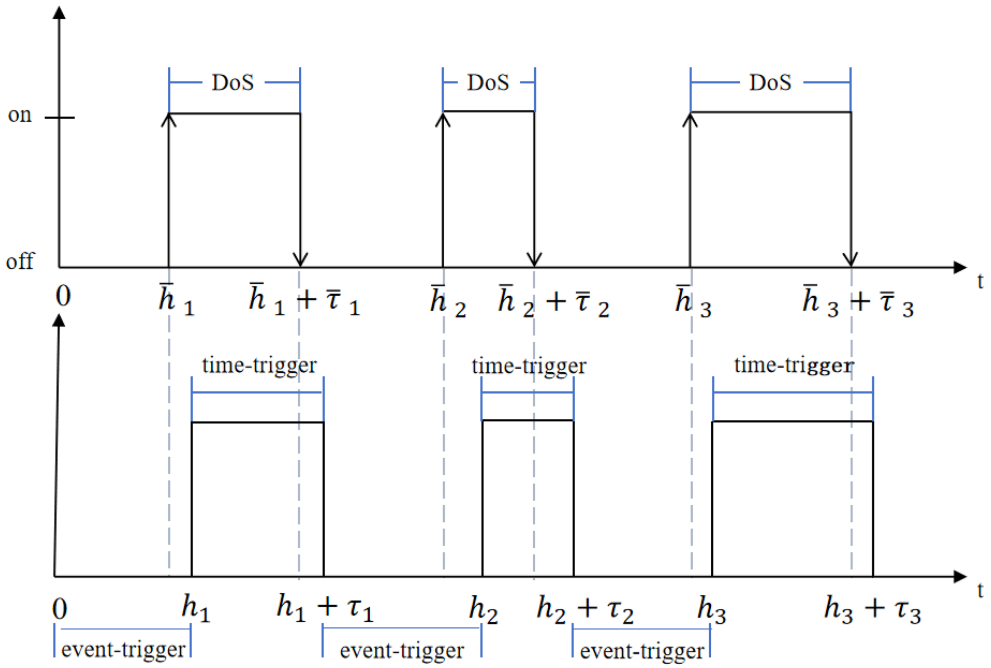

图 1　(网络版彩图) 混合采样机制示意图.

Figure 1　(Color online) The hybrid sampling mechanism.

即最近一次成功更新的控制量与当前控制量之间的差. 定义基于时间采样的间隔为 δ_0, 满足 $\tau_m \leqslant \delta_0 \leqslant \Delta_s$, 其中 τ_m 为最小更新时间间隔, Δ_s 为采样间隔上界. 基于事件触发机制的采样间隔定义为

$$\delta_k = \inf\left\{ t > t_k + \tau_m \;\middle|\; \|u_s(t)\| - \sigma\|z(t)\| \geqslant 0 \right\}, \tag{14}$$

其中, $\sigma > 0$ 为设计参数. 由于式 (14) 在定义事件触发机制时引入最小触发间隔 τ_m, 从而对任意 k 都有 $t_{k+1} - t_k \geqslant \tau_m > 0$, 且 τ_m 为提前给定的硬件平台固定属性, 因此可排除有限时间内的无限次触发, 并在保证无 Zeno 现象的同时维持较低通信更新频率.

则混合采样机制下采样序列 $\{t_k\}_{k\in\mathbb{N}}$ 的更新规则为

$$t_{k+1} = \begin{cases} t_k + \delta_0, & k \in \Omega, \\ t_k + \delta_k, & k \notin \Omega, \end{cases} \tag{15}$$

其中, $\Omega = \{k \in \mathbb{N} : t_k \in \bigcup_{p\in\mathbb{N}^+} H_p\}$ 表示受攻击时间序列的集合. 式 (15) 并非简单在两种采样方式之间切换, 而是通过集合 Ω 将 DoS 时序与采样规则相结合, 使更新与攻击段的可通信窗口同步, 从而便于后续对采样误差进行分段估计. 式 (15) 表示的混合采样机制示意图如图 1 所示.

4　问题可解性

本节首先证明问题 1 可通过控制律 (8) 和 (12) 求解, 其中采样时间序列 $\{t_k\}_{k\in\mathbb{N}}$ 则由式 (15) 确定. 由于进行了坐标变换, 参考引理 1 [18] 来建立受限状态 x 与无约束状态 z 之间的关系. 则对于 $x(T_1) \in S_s$, 其中 S_s 由式 (3) 给出, 且 $0 \leqslant T_1 < +\infty$, 如果状态 z 满足 $||z(x(t))|| \leqslant z_m$, $\forall t \in [T_1, T_2)$, $z_m = \mu(k_c - k_{c0})(k_c - k_{c0})$, 对于 $T_1 < T_2 \leqslant +\infty$, 那么对于所有 $t \in [T_1, T_2)$, 都有 $x(t) \in S_s$.

为便于表述, 定义

$$\begin{aligned} &z_0 = \mu(k_c - \bar{k}_{c0})(k_c - \bar{k}_{c0}),\\ &\kappa_* = \kappa + (1+\xi)\tau_m, \quad T_* = \frac{\tau_D T}{\tau_D + T\tau_m}. \end{aligned} \tag{16}$$

接下来, 通过定理 1 对上述控制方案的收敛性与稳定性进行说明.

定理1　考虑 DoS 攻击满足假设 1 和 2 以及 $M_0 = (\Delta_s/\tau_D) + (1/T) < 1$. 在假设 3 下, 对于非线性系统 (1), 若初始状态满足 $x(0) \in S_I$, 且 $z_m > z_0$, 问题 1 可通过控制器 (8) 和 (12) 与混合采样机制 (15) 来求解, 其中关键控制参数需满足以下条件:

$$m_1 > \frac{M_0 m_2}{1 - M_0}, \tag{17a}$$

$$Q(x) \geqslant \|\rho\|\gamma(x), \tag{17b}$$

$$m_2 > \max_{x(t)\in S_s}\{Q(x)\}, \tag{17c}$$

$$P(x) \geqslant 2\|\rho\|\gamma(x) + 2\mu\|\rho\|b_M\sigma, \tag{17d}$$

$$v_j \leqslant \frac{2}{m_2}\ln\frac{z_m}{z_0} + \frac{m_1}{m_2}\big|\Theta(0,\zeta_j)\big| - \big|\Xi(0,\zeta_j)\big|, j \in \mathbb{N}, \tag{17e}$$

$$\tau_m \leqslant \delta_0 \leqslant \Delta_s < \tau_D\left(\frac{m_1}{m_1+m_2} - \frac{1}{T}\right). \tag{17f}$$

证明　首先不失一般性, 令 $\zeta_0 = 0$. 由 $x(0) \in S_I$ 及系统的连续性可知, 存在 $0 \leqslant v_0^* < v_0$ 使得 $x(t) \in S_s$ 对所有 $t \in [\zeta_0, \zeta_0 + v_0^*)$ 成立. 构造 Lyapunov 函数为

$$V = \frac{1}{2}z^{\mathrm{T}}z. \tag{18}$$

沿系统轨迹对 $V(t)$ 求导可得

$$\dot{V} = z^{\mathrm{T}}\dot{z} = z^{\mathrm{T}}(\mu\rho g(x,w)) \leqslant \|\rho\|\gamma(x)\|z\|^2.$$

由式 (17c) 及 (17b) 得到

$$\|z(t)\|^2 \leqslant 2e^{m_2(t-\zeta_0)}V(\zeta_0) \leqslant e^{m_2(t-\zeta_0)}\|z(\zeta_0)\|^2.$$

根据式 (16) 及 $t - \zeta_0 \leqslant {v_0}^*$ 可知

$$\|z(t)\| \leqslant e^{\frac{m_2}{2}{v_0}^*}z(\zeta_0).$$

令 $v_0^* \triangleq \frac{2}{m_2}\ln\frac{z_m}{z_0}$, 当时间间隔满足 $v_0 \leqslant v_0^*$ 时, 系统状态在 $[\zeta_0, \zeta_0 + v_0)$ 内始终满足约束, 即 $x(t) \in S_s$ 恒成立, 从而得到

$$\dot{V} \leqslant m_2 V,\ t \in [\zeta_0, \zeta_0 + v_0)\,. \tag{19}$$

进一步, 由于 $|\Xi(0,t)| = t - \zeta_0$ 与 $|\Theta(0,t)| = 0$, 则

$$V(t) \leqslant e^{m_2(t-\zeta_0)}V(0) = e^{-m_1|\Theta(0,t)|}e^{m_2|\Xi(0,t)|}V(0). \tag{20}$$

其次, 在系统中没有发生 DoS 攻击的时段 $t \in [\zeta_0 + v_0, \zeta_1)$, 对李雅普诺夫函数 $V(t)$ 求导可以推导出

$$\begin{aligned} \dot{V} &= z^{\mathrm{T}}\dot{z} = z^{\mathrm{T}}\mu\rho(g(x,w) + bu_0 + bu_s)\\ &\leqslant \|\rho\|\gamma(x)\|z\|^2 + \mu\|\rho\|b\sigma\|z\|^2 + z^{\mathrm{T}}\mu\rho bu_0\\ &\leqslant (\|\rho\|\gamma(x) + \mu\|\rho\|b\sigma)\|z\|^2 + z^{\mathrm{T}}\mu\rho bu_0. \end{aligned}$$

由式 (17d) 及控制器 (12) 可以得到

$$\dot{V} \leqslant -m_1 V. \tag{21}$$

对于 $t \in [\zeta_0 + v_0, \zeta_1)$, 由于 $|\Theta(0,t)| = t - \zeta_0 - v_0$ 与 $|\Xi(0,t)| = v_0$, 可得

$$\begin{aligned} V(t) &\leqslant e^{-m_1(t-\zeta_0-v_0)} V(\zeta_0 + v_0) \\ &\leqslant e^{-m_1(t-\zeta_0-v_0)} e^{m_2 v_0} V(0) \\ &= e^{-m_1|\Theta(0,t)|} e^{m_2|\Xi(0,t)|} V(0). \end{aligned} \tag{22}$$

由此可得, 当 $t \in [\zeta_0 + v_0, \zeta_1)$ 时 $x(t) \in S_s$.

综上所述, 结合式 (22) 可知, 对所有 $t \in [0, \zeta_1)$, 约束 $x(t) \in S_s$ 均成立, 且满足如下不等式:

$$\dot{V}(t) \leqslant \begin{cases} m_2 V(t), & t \in [\zeta_0, \zeta_0 + v_0), \\ -m_1 V(t), & t \in [\zeta_0 + v_0, \zeta_1), \end{cases} \tag{23}$$

$$V(t) \leqslant e^{-m_1|\Theta(0,t)|} e^{m_2|\Xi(0,t)|} V(0). \tag{24}$$

对任意 $j \in \mathbb{N} \setminus \{0\}$, 考虑 $t \in [\zeta_j, \zeta_{j+1})$, 假设式 (23) 在 $[0, \zeta_j)$ 成立且 $x(t) \in S_s$. 由系统连续性可知, 存在 $v_j^* > 0$ 使得 $t \in \left[\zeta_j, \zeta_j + v_j^*\right)$ 时 $\dot{V} \leqslant m_2 V$, 且

$$V(t) \leqslant e^{m_2(t-\zeta_j)} V(\zeta_j). \tag{25}$$

结合式 (23) 可知

$$V(\zeta_j) \leqslant e^{-m_1|\Theta(0,\zeta_j)|} e^{m_2|\Xi(0,\zeta_j)|} V(0). \tag{26}$$

将其代入式 (25), 可得

$$V(t) \leqslant e^{m_2(t-\zeta_j)} e^{-m_1|\Theta(0,\zeta_j)|} e^{m_2|\Xi(0,\zeta_j)|} V(0). \tag{27}$$

由式 (16) 与 (27) 得

$$\|z(t)\| \leqslant e^{-\frac{m_1}{2}|\Theta(0,\zeta_j)|} e^{\frac{m_2}{2}(t-\zeta_j+|\Xi(0,\zeta_j)|)} z_0.$$

令 $v_j \leqslant v_j^* = \frac{2}{m_2} \ln \frac{z_m}{z_0} + \frac{m_1}{m_2} |\Theta(0,\zeta_j)| - |\Xi(0,\zeta_j)|$, 则有

$$\|z(t)\| \leqslant z_m. \tag{28}$$

结合 $|\Theta(0,t)|$ 与 $|\Xi(0,t)|$ 的关系推导出

$$V(t) \leqslant e^{-m_1|\Theta(0,t)|} e^{m_2|\Xi(0,t)|} V(0). \tag{29}$$

通过类似式 (21) 的证明过程可知, 在 $t \in [\zeta_j + v_j, \zeta_{j+1})$ 上

$$\dot{V}(t) \leqslant -m_1 V(t). \tag{30}$$

结合式 (25) 与 (30) 可以得到

$$\begin{aligned} V(t) &\leqslant e^{-m_1(t-\zeta_j-v_j)} V(\zeta_j + v_j) \\ &\leqslant e^{-m_1(t-\zeta_j-v_j)} e^{m_2(\zeta_j+v_j-\zeta_j)} V(\zeta_j) \\ &\leqslant e^{-m_1(t-\zeta_j-v_j)} e^{m_2 v_j} e^{-m_1|\Theta(0,\zeta_j)|} e^{m_2|\Xi(0,\zeta_j)|} V(0) \\ &= e^{-m_1(t-\zeta_j-v_j+|\Theta(0,\zeta_j)|)} e^{m_2(v_j+|\Xi(0,\zeta_j)|)} V(0). \end{aligned} \tag{31}$$

因此, 系统状态 $\|z(t)\|$ 随时间呈指数衰减, 并在 $t\in[\zeta_j+v_j,\zeta_{j+1})$ 内始终满足预设状态约束 $x(t)\in S_s$. 在此基础上, 进一步推导闭环解的安全性. 由障碍函数坐标变换及文献 [18] 中的等价关系可知, 如果无约束变量 $z(t)$ 在 $[0,+\infty)$ 上有界, 则受限状态 $x(t)$ 始终满足 $x(t)\in S_s$, 从而不触及约束边界. 在假设 1 和 2 所给的 DoS 攻击强度约束下, 结合初始条件 $x(0)\in S_I$ 以及已证明的 $V(t)\to 0$, 可得 $z(t)$ 有界并收敛, 因而轨迹始终位于 $S_s\subset S$ 内, 安全性结论成立.

最后, 证明 $\lim_{t\to\infty}x(t)=0$, 即在 $t\to\infty$ 时, 系统的状态可收敛到零.

注意到 $\Xi(\tau,t)$ 的上界可由 DoS 攻击的持续时长和 Δ 确定, 在假设 1 和 2 下有

$$\begin{aligned}|\Xi(\tau,t)|&\leqslant|\bar{\Xi}(\tau,t)|+(1+n(\tau,t))\tau_m\\&\leqslant\kappa+\frac{t-\tau}{T}+\left(1+\xi+\frac{t-\tau}{\tau_D}\right)\tau_m=\kappa_*+\frac{t-\tau}{T_*},\end{aligned}\tag{32}$$

其中, κ_* 和 T_* 由式 (16) 定义. 通过式 (24) 及假设 1 推导出

$$V(t)\leqslant e^{\kappa_*(m_1+m_2)}e^{-\left(m_1-\frac{m_1+m_2}{T_*}\right)t}V(0).\tag{33}$$

由式 (17f) 可知, $m_1-\frac{m_1+m_2}{T_*}>0$, 故可以得到式 (33) 满足 $\lim_{t\to\infty}V(t)=0$, 通过式 (9) 可得 $\mu(\cdot)$ 有界, 因此, 由式 (10) 得到系统状态满足 $\lim_{t\to\infty}x(t)=0$, 系统半全局渐近稳定.

5　仿真验证

考虑一个非线性系统

$$\dot{x}(t)=\begin{bmatrix}x_2\\-x_1+wx_2(1-{x_1}^2)\end{bmatrix}+u(t),\tag{34}$$

其中, $x=\mathrm{col}(x_1,x_2)\in\mathbb{R}^2$ 为状态, $u=\mathrm{col}(u_1,u_2)\in\mathbb{R}^2$ 为控制器. 系统状态初始值为 $x(0)=\mathrm{col}(0.8,-0.4)$, 选择控制系数为 $b_m=0.2$, $b_M=2$. 接着, 针对双重安全控制器 (8) 和 (12) 设计非线性函数

$$P(x)=10\big(x^2+1\big).\tag{35}$$

设置扰动参数和事件触发参数分别为 $w=0.8$, $\sigma=0.2$, 采样时间 $\tau_m=0.001$ s, $\delta_0=0.002$ s. 状态约束参数设为 $k_c=1.5$, $k_{c0}=0.01$, $\bar{k}_{c0}=0.2$. 此外, 系统 (34) 还受到了随机发生的 DoS 攻击, 选择 DoS 攻击的参数为 $\xi=1$, $\tau_D=0.5$, $\kappa=0.05$, $T=4$, 设定 DoS 攻击将在 0.25, 1.80, 3.60, 5.30, 6.40, 7.75, 8.65, 9.70 s 发生. 参考上述参数设计, 对基于控制律 (8) 和 (12) 的闭环系统性能通过数值仿真加以验证, 相关结果如图 2∼4 所示.

如图 2 所示, 灰色阴影区域表示随机 DoS 攻击的持续时间, 其时长及频率符合假设 1 及 2. 在攻击发生初期, 由于系统初始状态偏离稳态, 因此状态 x_1 与 x_2 出现轻微偏离, 但在所设计控制律作用下始终保持在约束区间内, 未发生越界; 当攻击结束后, 状态迅速恢复闭环稳定性并收敛至零点. 红色实线与蓝色虚线分别表示 x_1 与 x_2 的轨迹, 其峰值被快速抑制, 且在 DoS 发生导致的通信中断期间未出现误差积累.

由图 3 可见, 系统状态的范数 $\|x(t)\|$ 在初始阶段经历短暂过渡后迅速衰减, 并稳定于平衡点附近. 且 $\|x(t)\|$ 始终处于约束边界内, 红色虚线表示对状态的约束边界, 验证了控制律对状态约束的有效保持能力. 同时, 在随机扰动与攻击作用下, 状态收敛速度较快, 表明控制器仍能保证非线性系统的有界性与渐近稳定性.

从图 4 可见, 正常通信阶段触发间隔逐步增大, 表明误差收敛, 状态趋于平稳. 图中灰色竖向阴影条表示 DoS 攻击区间, 此时控制端信息无法到达执行器, 触发策略切换为时间触发更新. 此时, 采样时间间隔显著缩短, 控制信号以固定频率更新, 表现为蓝色柱状序列更为密集, 即 $t_{k+1}-t_k$ 受上界约束并保持较小取值. 攻击结束后, 控制器快速恢复基于事件触发的采样模式, 使采样间隔回到正常水平. 整体结果表明, 该混合触发策略在保证稳定性的同时有效降低通信负载, 并在攻击条件下仍能维持良好的鲁棒性与自适应切换能力.

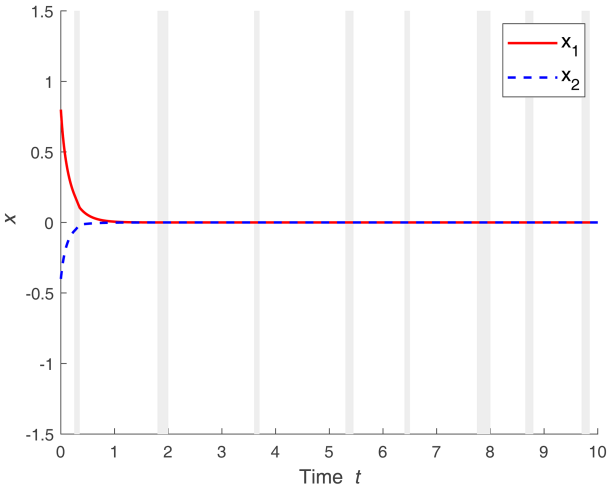

图 2　(网络版彩图) 状态轨迹 $x=\mathrm{col}(x_1,x_2)$.

Figure 2　(Color online) State trajectory $x=\mathrm{col}(x_1,x_2)$.

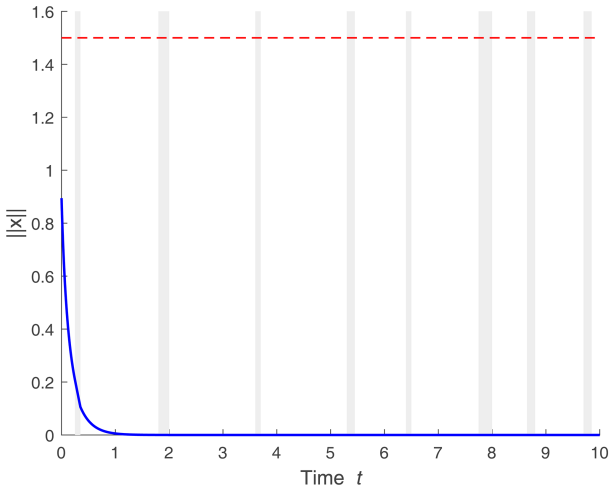

图 3　(网络版彩图) $\|x\|$ 轨迹.

Figure 3　(Color online) $\|x\|$ trajectory.

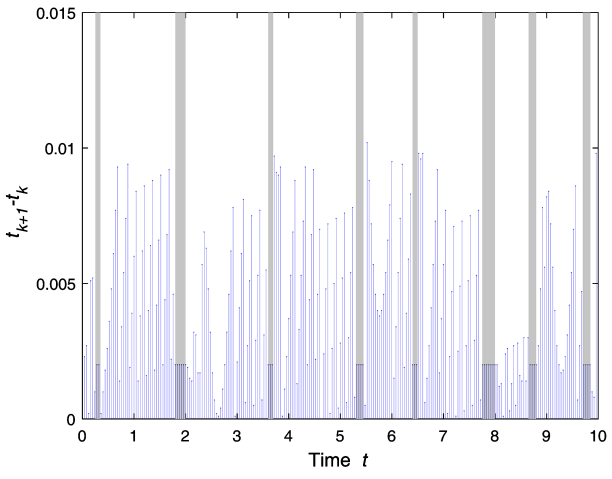

图 4　(网络版彩图) 采样时间间隔 $t_{k+1}-t_k$.

Figure 4　(Color online) Sampling time interval $t_{k+1}-t_k$.

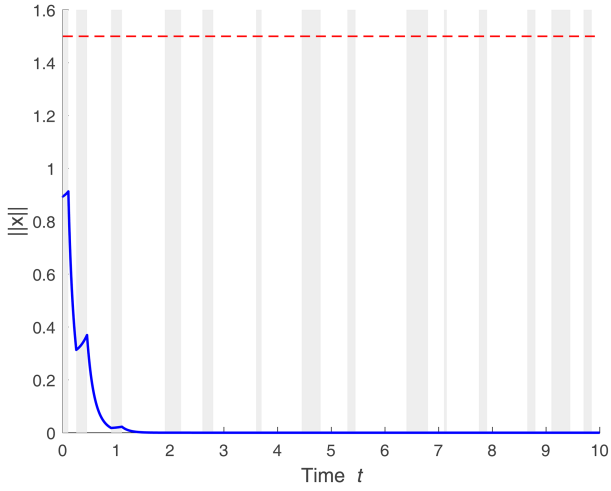

图 5　(网络版彩图) 改变攻击下的 $\|x\|$ 轨迹.

Figure 5　(Color online) $\|x\|$ trajectory under different attacks.

为检验所提方法在不同 DoS 攻击强度下的有效性, 本文在仿真中改变了 DoS 攻击的发生频率以及单次攻击的持续时长与总发生次数, 如图 5 所示. 可以观察到, 闭环系统在攻击窗口内的信息更新受到抑制, 导致状态收敛过程相较于无攻击或弱攻击情形更为缓慢, $\|x(t)\|$ 的衰减速度降低并出现更长的过渡阶段. 但在整个仿真时域内 $\|x(t)\|$ 始终保持在安全边界以下, 并在攻击结束后能够继续下降并最终收敛至邻域内, 表明所设计的控制器能够在攻击频率与时长变化条件下仍维持安全性与稳定性.

为验证所提方法在 DoS 攻击环境下的安全性与稳定性, 本文将所提出的控制设计与文献 [22] 中的仅抗 DoS 攻击跟踪控制器进行对比, 结果如图 6 所示. 可以观察到, 相较于本文方法的控制器, 该控制器闭环响应变慢, $\|x(t)\|$ 衰减速率降低并出现更长的过渡过程; 但在整个仿真时域内 $\|x(t)\|$ 始终低于安全边界. 相比之下, 仅抗攻击的控制器 [22] 虽可在一定程度上抑制 DoS 并使 $\|x(t)\|$ 总体下降, 但由于未显式嵌入安全约束, 难以对安全边界提供严格保证.

进一步地, 本文将所提方法与文献 [23] 中的仅考虑状态受限的安全攸关控制器进行对比. 图 7 给出了该控

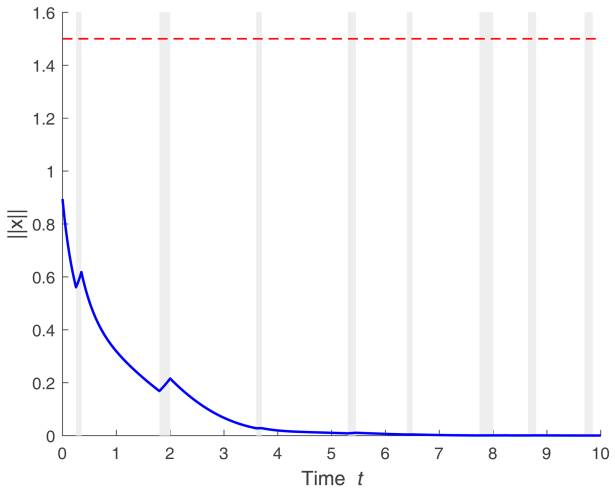

图 6　(网络版彩图) 文献 [22] 中控制器下的 $\|x\|$ 轨迹.

Figure 6　(Color online) $\|x\|$ trajectory under the controllor in [22].

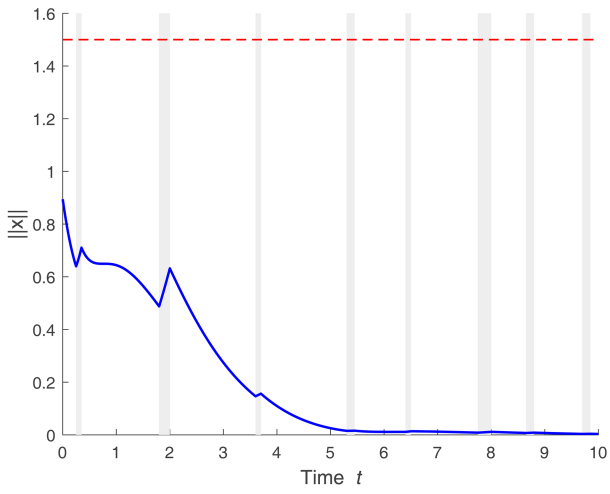

图 7　(网络版彩图) 文献 [23] 中控制器下的 $\|x\|$ 轨迹.

Figure 7　(Color online) $\|x\|$ trajectory under the controllor in [23].

制器的仿真结果. 可以看到, 在随机 DoS 攻击作用下, 系统在攻击窗口附近出现更明显的波动与收敛变慢, 闭环性能对通信中断较为敏感, 从而使系统性能受到影响. 上述结果表明, 单纯抗攻击控制难以保证安全约束的严格满足, 而单纯安全关键控制又难以在 DoS 条件下维持期望的鲁棒性与收敛性能; 所提方法能够实现安全性与抗攻击鲁棒性的统一.

综上, 仿真结果充分验证了结合混合触发机制与障碍函数方法的控制方案在非周期性随机 DoS 攻击下的强鲁棒性与约束保持能力, 为其在更高维复杂或多体系统中的推广应用提供了理论依据与方法支持.

6　总结

本文主要研究了随机 DoS 攻击下状态受限的非线性系统网络安全镇定问题. 为有效应对网络攻击带来的随机性和不确定性挑战, 本文提出了一种融合时间触发机制与事件触发机制的混合采样控制策略. 该策略在保证系统状态约束不被破坏的前提下, 通过灵活调度采样方式实现对系统通信资源的合理分配. 并且采用障碍函数方法将受限系统转换为无约束的系统进行控制器设计, 从而构建出具有较强鲁棒性的控制框架. 在理论上, 本文通过严格的稳定性与可行性分析, 证明了所提方法能够在攻击发生的概率和持续时间变化的情形下, 有效削弱不确定性对系统的负面影响, 保证系统状态能够逐步收敛至期望平衡点. 数值仿真验证的结果进一步表明, 该方法不仅能够在未知 DoS 攻击下保持系统稳定性能, 还能在降低采样频率和通信开销的同时, 有效维持系统在 DoS 攻击下的容错性, 从而兼顾了状态约束、网络安全与资源利用效率.

展望未来的研究方向, 可以进一步将本文提出的混合采样方法扩展应用到更高维度、耦合关系更复杂的非线性系统之中, 例如具有输入饱和特性、时变不确定参数或者存在时滞的复杂系统. 此外, 还可以考虑更具挑战性的多类网络攻击协同场景, 例如拒绝服务攻击与数据篡改、欺骗攻击等的组合, 或者引入复杂的网络时延模型进行分析. 与此同时, 将该方法推广至分布式与多智能体系统架构, 研究在受限通信条件下的协同网络安全控制与资源调度问题, 也将成为进一步提升该方法适用性与整体鲁棒性的关键研究方向.

参考文献

1　Lun Y Z, D'Innocenzo A, Smarra F, et al. State of the art of cyber-physical systems security: an automatic control perspective. J Syst Software, 2019, 149: 174–216

2 Duo W, Zhou M C, Abusorrah A. A survey of cyber attacks on cyber physical systems: recent advances and challenges. IEEE CAA J Autom Sin, 2022, 9: 784–800

3 Rezaee H, Abdollahi F. A decentralized cooperative control scheme with obstacle avoidance for a team of mobile robots. IEEE Trans Ind Electron, 2013, 61: 347–354

4 Gu N, Wang D, Peng Z, et al. Safety-critical containment maneuvering of underactuated autonomous surface vehicles based on neurodynamic optimization with control barrier functions. IEEE Trans Neural Netw Learn Syst, 2023, 34: 2882–2895

5 Wu C, Fang H, Yang Q, et al. Distributed cooperative control of redundant mobile manipulators with safety constraints. IEEE Trans Cybern, 2023, 53: 1195–1207

6 Persis C D, Tesi P. Input-to-state stabilizing control under denial of service. IEEE Trans Autom Control, 2015, 60: 2940–2955

7 Lu A Y, Yang G H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. IEEE Trans Automat Contr, 2018, 63: 1813–1820

8 Feng Z, Hu G. Secure cooperative event-triggered control of linear multiagent systems under DoS attacks. IEEE Trans Contr Syst Technol, 2020, 28: 741–752

9 Yang Y, Li Y, Yue D, et al. Distributed secure consensus control with event-triggering for multiagent systems under DoS attacks. IEEE Trans Cybern, 2021, 51: 2916–2928

10 Zhang Y, Feng G. Data-driven leader-following output consensus of discrete-time MASs under DoS attacks. Un Sys, 2025, 13: 1307–1318

11 Wang Y, Lu J, Liang J. Security control of multiagent systems under denial-of-service attacks. IEEE Trans Cybern, 2022, 52: 4323–4333

12 Liu Y, Deng C, Xie X, et al. Cooperative observer-based fuzzy tracking control for nonlinear MASs under DoS attacks. IEEE Trans Fuzzy Syst, 2024, 32: 767–777

13 Liu Y J, Tong S. Barrier Lyapunov Functions-based adaptive control for a class of nonlinear pure-feedback systems with full state constraints. Automatica, 2016, 64: 70–75

14 Zhao K, Song Y, Chen C L P, et al. Control of nonlinear systems under dynamic constraints: a unified barrier function-based approach. Automatica, 2020, 119: 109102

15 Zhao K, Song Y, Ma T, et al. Prescribed performance control of uncertain Euler-Lagrange systems subject to full-state constraints. IEEE Trans Neural Netw Learn Syst, 2018, 29: 3478–3489

16 Geng F, Dong Y, Hong Y. Unified barrier function based approach for practical fixed-time control of state-constrained nonlinear system. J Syst Sci Complex, 2025, 38: 782–804

17 Jiang Y, Niu B, Wang X, et al. Dynamic-estimator-based adaptive secure containment control for constrained nonlinear multi-agent systems under denial-of-service attacks. Intl J Robust Nonlinear, 2023, 33: 605–622

18 Dong Y, Hong Y, Chen J. Security control of safety-critical systems. IEEE Trans Cybern, 2025, 55: 2474–2485

19 Hespanha J, Morse A. Stability of switched systems with average dwell-time. In Proceedings of the 38th IEEE CDC, Orlando, 1999. 2655–2660

20 Cao Y, Wen C, Song Y. A unified event-triggered control approach for uncertain pure-feedback systems with or without state constraints. IEEE Trans Cybern, 2021, 51: 1262–1271

21 Chen Z, Huang J. Stabilization and Regulation of Nonlinear Systems: A Robust and Adaptive Approach. New York: Springer-Verlag, 2015

22 Kato R, Cetinkaya A, Ishii H. Linearization-based quantized stabilization of nonlinear systems under DoS attacks. IEEE Trans Automat Contr, 2022, 67: 6826–6833

23 Sabzalian M H. Safety-critical controller design for nonlinear systems: Stabilization and robustness. ISA Trans, 2025, 163: 98–107

Secure control of nonlinear systems under DoS attacks with state constraints

Ruolin SONG[1], Yiguang HONG[1,2], Yi DONG[1,2*], Bin XIN[3], Qing WANG[3] & Xi CHEN[4]

1. *Frontiers Science Center for Intelligent Autonomous Systems, Tongji University, Shanghai 201210, China*
2. *College of Electronic and Information Engineering, State Key Laboratory of Autonomous Intelligent Unmanned Systems, Ministry of Education, Tongji University, Shanghai 201804, China*
3. *School of Automation, Beijing Institute of Technology, Beijing 100081, China*
4. *Department of Mechanical and Automation Engineering, The Chinese University of Hong Kong, Hong Kong 999077, China*

* Corresponding author. E-mail: yidong@tongji.edu.cn

Abstract This paper investigates the secure stabilization problem for nonlinear systems subject to state constraints and denial of service (DoS) attacks. A hybrid sampling mechanism integrating time-triggered and event-triggered strategies is developed, based on which a class of safety and security controllers is designed via barrier functions. The proposed method can strictly enforce the prescribed state constraints while effectively reducing communication usage and exhibiting strong fault tolerance against DoS attacks. Theoretical analysis shows that the resulting closed-loop system is semi-globally asymptotically stable, which confirms the feasibility of the proposed control law in terms of both stability and robustness. Numerical simulations further demonstrate that, under DoS attacks with frequency and duration lying in certain ranges, the proposed method can rapidly suppress external disturbances and drive the system states to converge to the equilibrium point, thereby significantly improving the anti-disturbance capability and operational reliability of the system under DoS attacks.

Keywords denial of service attacks, nonlinear control, state constraints, barrier function, hybrid triggering