

文章编号: 1006-2467(2023)05-0624-07

DOI: 10.16183/j.cnki.jsjtu.2021.445

周期 DoS 攻击下变周期切换正系统的安全控制

刘 教, 孔祥娜, 张甜甜

(河北工业大学 人工智能与数据科学学院, 天津 300401)

摘 要: 周期拒绝服务(DoS)攻击阻止了切换正系统的测量通道与控制通道通过网络进行信息交换. 此外, 系统切换行为、DoS 攻击引起的混杂行为以及正性约束增加了安全控制研究的困难. 针对遭受周期 DoS 攻击的网络化切换正系统, 提出一种基于切换行为的建模方法并研究其安全控制问题. 在变周期切换条件下, 通过限定切换周期与 DoS 攻击周期的关系, 构造多线性余正 Lyapunov 函数, 并得到闭环系统为正系统以及渐近稳定条件, 进而基于正系统理论设计安全状态反馈控制器. 在此基础上, 讨论周期 DoS 攻击下系统进行恒定周期切换的情形. 最后, 通过仿真示例验证结果的有效性.

关键词: 切换正系统; 周期拒绝服务攻击; 多线性余正 Lyapunov 函数; 安全控制

中图分类号: TP 273

文献标志码: A

Secure Control for Variable Periodic Switched Positive Systems Under Periodic DoS Attack

LIU Jiao, KONG Xiangna, ZHANG Tiantian

(School of Artificial Intelligence, Hebei University of Technology, Tianjin 300401, China)

Abstract: Periodic denial-of-service (DoS) attack prevents the information exchange of measurement channel and control channel for switched positive systems through the network. Moreover, the coupling of system switching behavior and hybrid behavior due to DoS attack and positive constraint also increase the difficulty in secure control research. The secure control problem of networked switched positive systems under periodic DoS attack is studied and a modeling method based on switching behavior is proposed in this paper. Under variable periodic switching, the multiple linear copositive Lyapunov function is constructed to obtain the positive and asymptotically stable condition for the closed-loop system by limiting the relationship between the switching period and the DoS attack period, and a secure state feedback controller based on the positive system theory is designed, based on which, the constant periodic switching case is also discussed by using the positive system theory. Finally, the validity of the results is verified by a simulation example.

Key words: switched positive systems; periodic denial-of-service (DoS) attack; multiple linear copositive Lyapunov function; secure control

收稿日期: 2021-11-08 修回日期: 2021-12-29 录用日期: 2022-01-11

基金项目: 国家自然科学基金(62103129)资助项目

作者简介: 刘 教(1987-), 讲师, 现主要从事复杂系统控制、安全控制的研究, 电话(Tel.): 022-60203069; E-mail: jiaoliu@hebut.edu.cn.

网络化系统通过无线网络传输信息摆脱了地域限制,但无线网络的开放性使得系统完整性以及可用性遭受破坏,导致系统性能降低甚至失去稳定性.从网络安全控制的角度来说,网络攻击主要分为两类,一类是拒绝服务(DoS)攻击,另一类是欺骗攻击. DoS 攻击旨在阻断网络通信,破坏信息交换.如文献[1]中考虑了攻击者间歇发起 DoS 攻击以破坏测量通道数据可用性的情况.欺骗攻击则是通过在前向通道或反馈通道注入精心设计的错误数据,以破坏系统状态.如文献[2]中提出将欺骗攻击同时注入传感器到控制器的通道和控制器到执行器的通道来破坏系统完整性,进而探究网络系统的安全问题.相较于欺骗攻击, DoS 攻击是众多网络攻击中出现频率最高、危害最大、最易实现的攻击手段^[3-4].因此,近年来这方面研究成果较多^[5-6].

攻击者能量有限造成 DoS 攻击不能一直发生,因此,能量有限且方便实施的周期 DoS 攻击引起了学者们的广泛关注.文献[7-8]中研究了周期 DoS 攻击下网络系统的安全控制问题.文献[9]中将遭受周期 DoS 攻击的系统建模为切换系统,利用相对成熟的切换理论^[10-11]研究 DoS 攻击下系统的安全问题.但是对于遭受 DoS 攻击的切换系统而言,系统本身的切换特性与 DoS 攻击引起的切换特性相互耦合,这将导致混杂问题难以处理.针对此问题许多学者进行了研究,文献[12]中提出限制 DoS 攻击的持续区间以及发生频率,通过构造满足平均驻留时间的切换信号,以稳定遭受 DoS 攻击的切换系统.文献[13]中采取合适的事件触发机制将 DoS 攻击下的网络化切换系统建模为新型切换系统,实现安全控制.

另外,由于实际生活中常存在取值为非负的特殊物理量,例如细菌群落数量、森林覆盖率以及有机物浓度等,将这类物理量作为状态变量可得正系统.与一般系统不同,正系统是指初始状态和系统输入都为非负时,任意时刻的系统状态与输出都能保持非负的动态系统.近年来,描述特定切换法则、掌管模态切换的一类正系统被称为切换正系统,由于该系统具有可靠性强、应用范围广等优点,受到学者们的关注^[14-15],常应用于通信系统^[16]、编队飞行^[17]、流行病学^[18]等不同领域.对于遭受 DoS 攻击的切换正系统,DoS 攻击阻止了测量通道与控制通道之间的信息传递,导致系统稳定性及正性均受影响.同时系统状态的非负特性、子系统之间切换特性及 DoS 攻击引起的切换特性相互耦合,这更增加了问题解决的难度.因此,在遭受 DoS 攻击情形下,设计一种

安全控制器使得切换正系统依然能够保证其正性及稳定性尤为重要.目前,针对遭受 DoS 攻击的切换正系统的研究鲜有成果.

基于以上讨论,本文主要研究在周期 DoS 攻击及变周期切换信号下,网络化切换正系统的安全控制问题.研究过程中面临如下挑战,首先,系统的正性约束使得二次型 Lyapunov 方法体系中的线性矩阵不等式等理论均不再适用,需要寻找新的研究方法.其次,需要对周期 DoS 攻击下变周期切换正系统的切换行为进行建模.最后,需要考虑子系统之间切换特性和 DoS 攻击引起的切换特性相互耦合对安全控制造成的影响.

1 问题描述及预备知识

考虑如下切换系统:

$$\dot{x}(t) = A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t) \tag{1}$$

式中: $x(t) \in \mathbb{R}^n, u(t) \in \mathbb{R}^m$ 分别表示系统状态与控制输入; $\sigma(t): [0, \infty) \rightarrow M = \{1, 2, \dots, N\}$ 为系统切换信号, N 表示子系统个数.当第 l 个子系统被激活时,切换信号 $\sigma(t) = l$,对应的参数矩阵为 $A_l \in \mathbb{R}^{n \times n}, B_l \in \mathbb{R}^{n \times m}, A_l$ 为 Metzler 矩阵.

为保证系统(1)的正性及稳定性,设计如下状态反馈控制器:

$$u(t) = K_{\sigma(t)}x(t) \tag{2}$$

式中: $K_{\sigma(t)}$ 为待设计状态反馈控制器增益矩阵.

网络化切换正系统的控制信道和测量信道通过开放共享的无线网络传递信息,因此信息在传输过程中易因遭受 DoS 攻击而无法正常更新.故以切换正系统为研究对象,在传感器到控制器以及控制器到执行器之间的通道通过共享网络传递信息的情况下,设计 DoS 攻击下网络化切换正系统框架,如图 1 所示.

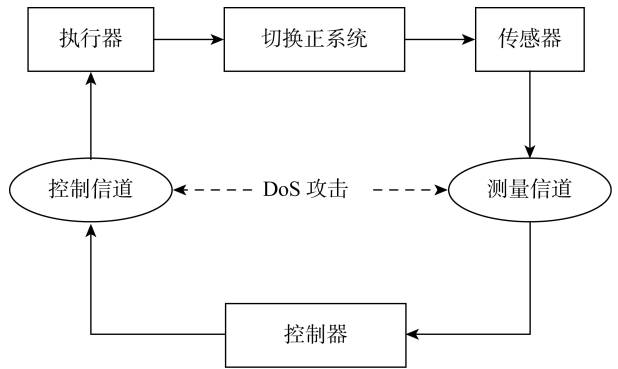


图 1 DoS 攻击下网络化切换正系统框架
Fig. 1 Architecture of networked switched positive system under DoS attack

假设 DoS 攻击同时作用于控制信道和测量信道. DoS 攻击及切换信号分别满足下列两个假设.

假设 1: DoS 攻击的周期恒定, 一个完整 DoS 攻击周期固定为 T_{DoS} .

假设 2: 切换信号的周期是变化的, 第 k 个切换区间的长度 T_k 与 DoS 攻击周期 T_{DoS} 关系为 $T_k = m_k T_{\text{DoS}}$, $m_k \in \{1, 2, \dots, m_{\max}\}$, 其中 m_k 为 DoS 攻击周期个数.

切换正系统遭受周期 DoS 攻击时, 切换信号与 DoS 攻击信号 $S_{\text{DoS}}(t)$ 关系如图 2 所示. 其中, 序列 $\{t_{k-1}, t_k, t_{k+1}, \dots\}$ 表示系统切换时刻. 假设在区间 $[t_{k-1}, t_k)$ 内, 为第 i 个子系统运行; 在区间 $[t_k, t_{k+1})$ 内, 为第 j 个子系统运行, 期间有 m_k 个 DoS 攻击周

期; 序列 $\{t_k, t_k + T_{\text{DoS}}, \dots, t_k + (m_k - 1)T_{\text{DoS}}\}$ 分别表示 DoS 攻击周期的起始时刻. 每个 DoS 攻击周期分为长度为 T_{off} 的休眠期和长度为 $T_{\text{DoS}} - T_{\text{off}}$ 的激活期. DoS 攻击信号 $S_{\text{DoS}}(t)$ 满足:

$$S_{\text{DoS}}(t) = \begin{cases} 1, & t \in [t_k + (\kappa - 1)T_{\text{DoS}}, \\ & t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}) \\ 0, & t \in [t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}, \\ & t_k + \kappa T_{\text{DoS}}) \end{cases} \quad (3)$$

式中: $\kappa \in \{1, 2, \dots, m_k\}$ 为 DoS 攻击周期次序. $S_{\text{DoS}}(t) = 1$ 表示 DoS 攻击处于休眠期, 此时进行正常通信; $S_{\text{DoS}}(t) = 0$ 表示 DoS 攻击处于激活期, 此时通信中断. 周期 DoS 攻击下执行器的输出^[19]可表

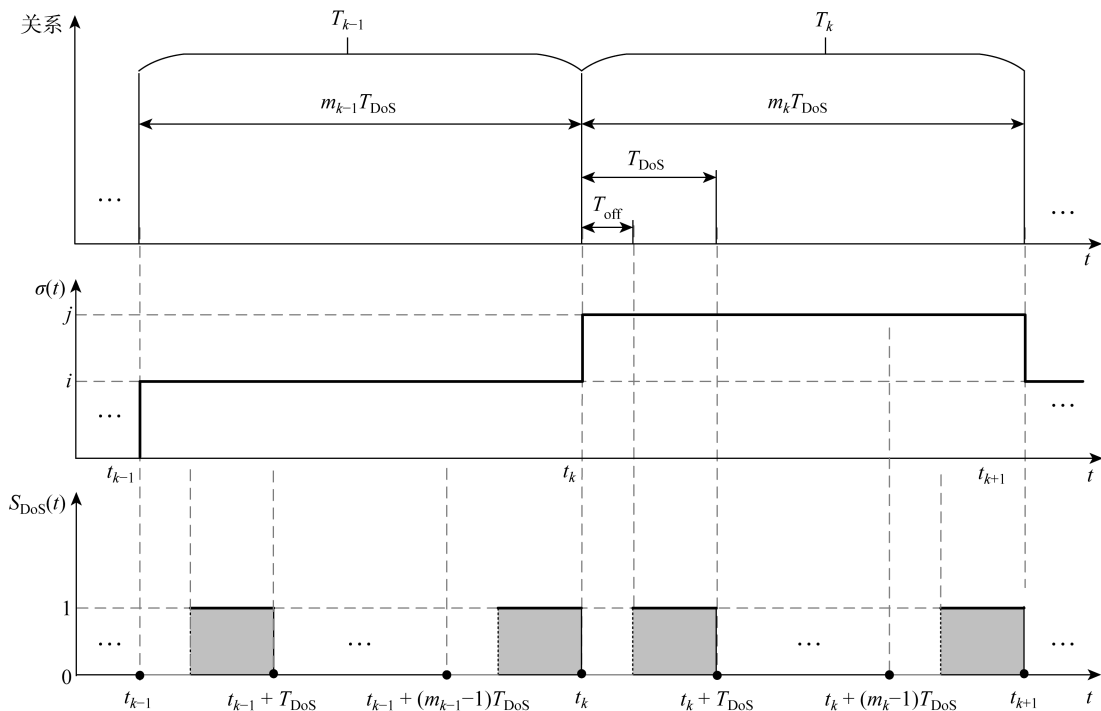


图 2 切换信号 $\sigma(t)$ 与 DoS 攻击信号 $S_{\text{DoS}}(t)$ 关系图

Fig. 2 Relationship between system switching signal $\sigma(t)$ and DoS attack signal $S_{\text{DoS}}(t)$

示为

$$u(t) = \begin{cases} K_{\sigma(t)} x(t), & S_{\text{DoS}}(t) = 1 \\ 0, & S_{\text{DoS}}(t) = 0 \end{cases} \quad (4)$$

根据式(1)、(3)和(4)可得遭受周期 DoS 攻击的闭环系统为

$$\dot{x}(t) = \begin{cases} A_{\sigma(t)} x(t) + B_{\sigma(t)} K_{\sigma(t)} x(t), \\ t \in [t_k + (\kappa - 1)T_{\text{DoS}}, \\ t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}) \\ A_{\sigma(t)} x(t), \\ t \in [t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}, t_k + \kappa T_{\text{DoS}}) \end{cases} \quad (5)$$

2 稳定性分析及控制器设计

给出在周期 DoS 攻击下闭环系统的稳定性条件并设计相应的安全控制器.

定理 1 对于系统(5), 给定常数 $\alpha > 0, \beta > 0, \mu > 1, s > 0, I$ 表示单位阵. 当 $i, j \in M$ 且 $i \neq j$ 时, 若存在向量 $p_j > 0$ 及矩阵 K_j 使得当 $\beta(T_{\text{DoS}} - T_{\text{off}}) \leq \alpha T_{\text{off}}$ 时, 式(6)~(10)成立, 或者当 $\beta(T_{\text{DoS}} - T_{\text{off}}) > \alpha T_{\text{off}}$ 时, 式(6)~(9)及(11)成立, 则系统(5)是正系统且渐近稳定, 其中“ $>$ ”或“ $<$ ”表示向量中每个元素都有大于或小于关系.

$$\mathbf{A}_j + \mathbf{B}_j \mathbf{K}_j + s\mathbf{I} > \mathbf{0} \quad (6)$$

$$(\mathbf{A}_j + \mathbf{B}_j \mathbf{K}_j)^\top \mathbf{p}_j + \alpha \mathbf{p}_j < \mathbf{0} \quad (7)$$

$$\mathbf{A}_j^\top \mathbf{p}_j - \beta \mathbf{p}_j < \mathbf{0} \quad (8)$$

$$\mathbf{p}_j < \mu \mathbf{p}_i \quad (9)$$

$$\left. \begin{aligned} \ln \mu + \beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}} &< 0 \\ \beta(T_{\text{DoS}} - T_{\text{off}}) &\leq \alpha T_{\text{off}} \end{aligned} \right\} \quad (10)$$

$$\left. \begin{aligned} \ln \mu + m_{\max}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}] &< 0 \\ \beta(T_{\text{DoS}} - T_{\text{off}}) &> \alpha T_{\text{off}} \end{aligned} \right\} \quad (11)$$

证明 由式(5)可知,在 DoS 攻击休眠期有 $\dot{\mathbf{x}}(t) = (\mathbf{A}_{\sigma(t)} + \mathbf{B}_{\sigma(t)} \mathbf{K}_{\sigma(t)}) \mathbf{x}(t)$. 由 $\mathbf{A}_j + \mathbf{B}_j \mathbf{K}_j$ 为 Metzler 矩阵得此区间系统为正系统. 在 DoS 攻击激活期有 $\dot{\mathbf{x}}(t) = \mathbf{A}_{\sigma(t)} \mathbf{x}(t)$, 由 \mathbf{A}_j 为 Metzler 矩阵得此区间系统为正系统,因此系统(5)是正系统.

为证明系统渐近稳定性,选择如下多线性余正 Lyapunov 函数:

$$V_{\sigma(t)}(t) = \mathbf{x}^\top(t) \mathbf{p}_{\sigma(t)} \quad (12)$$

当 DoS 攻击处于休眠期,即 $t \in [t_k + (\kappa - 1)T_{\text{DoS}}, t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}]$ 时,沿着系统(5)的轨迹对式(12)求导有

$$\dot{V}_j(t) = \mathbf{x}^\top(t) (\mathbf{A}_j + \mathbf{B}_j \mathbf{K}_j)^\top \mathbf{p}_j \quad (13)$$

因而有

$$\begin{aligned} \dot{V}_j(t) + \alpha V_j(t) &= \\ \mathbf{x}^\top(t) [(\mathbf{A}_j + \mathbf{B}_j \mathbf{K}_j)^\top \mathbf{p}_j + \alpha \mathbf{p}_j] \end{aligned} \quad (14)$$

由不等式(7)知:

$$\dot{V}_j(t) < -\alpha V_j(t) \quad (15)$$

对不等式(15)在区间 $[t_k + (\kappa - 1)T_{\text{DoS}}, t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}]$ 内求积分得到:

$$\begin{aligned} V_j[t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}] &< \\ e^{-\alpha T_{\text{off}}} V_j[t_k + (\kappa - 1)T_{\text{DoS}}] \end{aligned} \quad (16)$$

当 DoS 攻击处于激活期,即 $t \in [t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}, t_k + \kappa T_{\text{DoS}}]$ 时,沿着系统(5)的轨迹对式(12)求导可得:

$$\dot{V}_j(t) - \beta V_j(t) = \mathbf{x}^\top(t) (\mathbf{A}_j^\top \mathbf{p}_j - \beta \mathbf{p}_j) \quad (17)$$

由不等式(8)知:

$$\dot{V}_j(t) < \beta V_j(t) \quad (18)$$

对不等式(18)在区间 $[t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}, t_k + \kappa T_{\text{DoS}}]$ 内求积分得:

$$\begin{aligned} V_j(t_k + \kappa T_{\text{DoS}}) &< \\ e^{\beta(T_{\text{DoS}} - T_{\text{off}})} V_j[t_k + (\kappa - 1)T_{\text{DoS}} + T_{\text{off}}] \end{aligned} \quad (19)$$

结合不等式(16)和(19),可得整个 DoS 攻击周期 Lyapunov 函数的变化关系为

$$V_j(t_k + \kappa T_{\text{DoS}}) <$$

$$e^{\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}} V_j[t_k + (\kappa - 1)T_{\text{DoS}}] \quad (20)$$

考虑整个切换区间 $[t_k, t_{k+1})$, 该切换区间内含有 m_k 个 DoS 攻击周期,可得:

$$V_{\sigma(t_k)}(t_{k+1}) < e^{m_k[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]} V_{\sigma(t_k)}(t_k) \quad (21)$$

由式(9)可得切换时刻 t_k 处 Lyapunov 函数的变化为

$$V_{\sigma(t_{k+1})}(t_{k+1}) \leq \mu V_{\sigma(t_k)}(t_{k+1}) \quad (22)$$

结合式(21)~(22)可得:

$$V_{\sigma(t_{k+1})}(t_{k+1}) \leq \mu e^{m_k[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]} V_{\sigma(t_k)}(t_k) \quad (23)$$

推广到 0 初始状态,可得:

$$V_{\sigma(t_k)}(t_k) \leq \mu^k e^{\sum_{\theta=0}^{k-1} m_{\theta,k}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]} V_{\sigma(0)}(0) \quad (24)$$

由于系统为变周期切换,第 k 个切换区间内含有的攻击周期数目 $m_{\theta,k}$ ($\theta = 0, 1, \dots, k-1$) 不同,所以需要式(24)中的 $\sum_{\theta=0}^{k-1} m_{\theta,k}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]$ 进行放缩,主要对 $\beta(T_{\text{DoS}} - T_{\text{off}})$ 与 αT_{off} 的大小进行讨论:

当 $\beta(T_{\text{DoS}} - T_{\text{off}}) \leq \alpha T_{\text{off}}$ 时,令 $\eta_1 = \ln \mu + \beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}$, 由 $m_{\theta,k} > 0$ 及式(10)可得:

$$\begin{aligned} V_{\sigma(t_k)}(t_k) &\leq e^{[\ln \mu + \beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]k} V_{\sigma(0)}(0) = \\ e^{\eta_1 k} V_{\sigma(0)}(0), \quad \eta_1 &< 0 \end{aligned} \quad (25)$$

当 $\beta(T_{\text{DoS}} - T_{\text{off}}) > \alpha T_{\text{off}}$ 时,令 $\eta_2 = \ln \mu + m_{\max}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]$, 由 $m_{\theta,k} < m_{\max}$ 及式(11)可得:

$$\begin{aligned} V_{\sigma(t_k)}(t_k) &\leq e^{[\ln \mu + m_{\max}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]]k} V_{\sigma(0)}(0) = \\ e^{\eta_2 k} V_{\sigma(0)}(0), \quad \eta_2 &< 0 \end{aligned} \quad (26)$$

令 $\eta = \max\{\eta_1, \eta_2\}$, 有 $V_{\sigma(t_k)}(t_k) \leq e^{\eta k} V_{\sigma(0)}(0)$ 且 $\eta < 0$. 因为每个 DoS 攻击周期内 Lyapunov 函数最大值在攻击结束的時刻得到,所以对于 $\forall t \in [t_k, t_{k+1})$ 有

$$\begin{aligned} V_{\sigma(t_k)}(t) &\leq \max_{\kappa \in 0, 1, \dots, m_k} e^{\kappa[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]} V_{\sigma(t_k)}(t_k) \leq \\ \max_{\kappa \in 0, 1, \dots, m_k} \{e^{[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]} &, e^{m_{\max}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]}\} \times \\ V_{\sigma(t_k)}(t_k) \end{aligned} \quad (27)$$

此外,令 $c = \max_{\kappa \in 0, 1, \dots, m_k} \{e^{\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}}, e^{m_{\max}[\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}]}\}$, 可得:

$$V_{\sigma(t_k)}(t) \leq c V_{\sigma(t_k)}(t_k) \leq c e^{\eta k} V_{\sigma(0)}(0) \quad (28)$$

由于

$$V_{\sigma(0)}(0) \leq \varepsilon_1 \|\mathbf{x}_{\sigma(0)}(0)\| \quad (29)$$

$$V_{\sigma(t)}(t) \leq \varepsilon_2 \|\mathbf{x}_{\sigma(t)}(t)\| \quad (30)$$

其中 $\varepsilon_1 = \max_{j \in M} p_j, \varepsilon_2 = \min_{j \in M} p_j$. 因此有

$$\|x_{\sigma(t)}(t)\| \leq \frac{\varepsilon_1}{\varepsilon_2} c e^{\eta(k+1)} \|x_{\sigma(0)}(0)\| \quad (31)$$

由 $c e^{\eta(k+1)} < 1$ 可以看出整个系统的能量呈现全局递减的趋势, 即系统全局渐近稳定.

定理 2 对于系统(5), 给定向量 \tilde{v}_j 和常数 $\alpha > 0, \lambda > 0, \mu > 1$, 若存在适当维数矩阵 z_j 和 p_j , 使得当 $\beta(T_{\text{DoS}} - T_{\text{off}}) > \alpha T_{\text{off}}$ 时, 式(8)~(10)及式(31)~(33)成立或者当 $\beta(T_{\text{DoS}} - T_{\text{off}}) < \alpha T_{\text{off}}$ 时, 式(8)~(9)和(11)及式(31)~(33)成立时, 则在控制器即式(34)的作用下, 系统(5)是正系统且渐近稳定.

$$\tilde{v}_j^T B_j^T p_j A_j + B_j \tilde{v}_j z_j^T + \lambda I > 0 \quad (32)$$

$$\tilde{v}_j^T B_j^T p_j > 0 \quad (33)$$

$$A_j^T p_j + z_j + \alpha p_j < 0 \quad (34)$$

$$u(t) = K_j x(t) = \frac{1}{\tilde{v}_j^T B_j^T p_j} \tilde{v}_j z_j^T x(t) \quad (35)$$

证明 在式(31)两侧同时除以式(32), 可得:

$$A_j + B_j \frac{1}{\tilde{v}_j^T B_j^T p_j} \tilde{v}_j z_j^T + \frac{\lambda}{\tilde{v}_j^T B_j^T p_j} I > 0 \quad (36)$$

令 $z_j = K_j^T B_j^T p_j, s = \frac{\lambda}{\tilde{v}_j^T B_j^T p_j}$, 代入式(35)有

$$A_j + B_j K_j + s I > 0 \quad (37)$$

另将 z_j 代入式(33)中, 可得:

$$A_j^T p_j + K_j^T B_j^T p_j + \alpha p_j < 0 \quad (38)$$

式(37)即转化为式(7), 此时结合定理 1 可得系统(5)为正系统且渐近稳定.

为求解控制器增益, 设计如下算法.

算法

1. 给定矩阵 A_j 与 B_j , 以及参数 $\alpha, \beta, \mu, T_{\text{DoS}}, T_{\text{off}}$ 的值并设定 \tilde{v}_j 的值.
2. 通过定理 1 获得切换正系统稳定性条件.
3. 根据定理 1 计算出 p_j 与 z_j 的数值.
4. 通过定理 2 设计出状态反馈控制器增益为

$$K_j = \frac{1}{\tilde{v}_j^T B_j^T p_j} \tilde{v}_j z_j^T$$

推论 1 在定理 1 中, 若 $m_k = \kappa$, 则对于式(5)所描述系统, 给定常数 $\alpha > 0, \beta > 0, \mu > 1, s > 0$, 若存在适当维数矩阵 $p_j > 0$ 和控制器增益 K_j , 常数 $\lambda > 0$ 和适当维数的矩阵 $z_j (j \in M)$, 使得式(6)~(9)和式(31)~(33)及下列不等式成立:

$$\ln \mu + \kappa [\beta(T_{\text{DoS}} - T_{\text{off}}) - \alpha T_{\text{off}}] < 0 \quad (39)$$

$$u(t) = K_j x(t) = \frac{1}{\tilde{v}_j^T B_j^T p_j} \tilde{v}_j z_j^T x(t) \quad (40)$$

则在控制器(39)的作用下, 系统(5)为正系统且渐近稳定.

3 仿真实例

考虑连续时间切换正系统(1)中含有如下两个子系统:

$$A_1 = \begin{bmatrix} -0.17 & 0.20 \\ 0 & -0.90 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 0.28 & 0.58 \\ 0.30 & 0.11 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} -0.14 & 0.34 \\ 0.06 & -0.70 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 0.16 & 0.31 \\ 0.69 & 0.35 \end{bmatrix}$$

选择 DoS 攻击信号的攻击周期 $T_{\text{DoS}} = 10$ s, 休眠期 $T_{\text{off}} = 6$ s, 给定初始条件 $x(0) = [1 \ 3]^T$. 考虑变周期切换, 即系统(1)的每个切换区间所受到的攻击次数不同, 选择 $m_{\text{max}} = 10, \alpha = 0.10, \beta = 0.10, \mu = 1.20, \lambda = 10.60, \tilde{v}_1 = [0.23 \ 0.19]^T, \tilde{v}_2 = [0.19 \ 0.3]^T$. 此时满足条件式(10), 由此可得控制器增益矩阵:

$$K_1 = \begin{bmatrix} 0.006 \ 2 & 0.006 \ 2 \\ 0.005 \ 8 & 0.005 \ 8 \end{bmatrix}$$

$$K_2 = \begin{bmatrix} 0.003 \ 5 & 0.003 \ 5 \\ 0.006 \ 9 & 0.006 \ 9 \end{bmatrix}$$

周期 DoS 攻击信号如图 3 所示. 此外在图 4 中, 系统共有 4 个切换区间, 但每个切换区间的长度不同, 每个子系统运行时受到的周期 DoS 攻击次数不同. 系统的状态轨迹曲线如图 5 所示, 即在受到周期 DoS 攻击情况下, 尽管系统为变周期切换, 仍可以在控制器的作用下趋于稳定且保持非负状态, 验证了定理 2 的有效性.

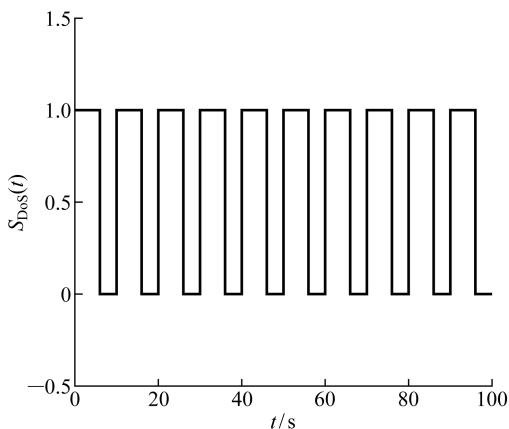


图 3 DoS 攻击信号

Fig. 3 DoS attack signal

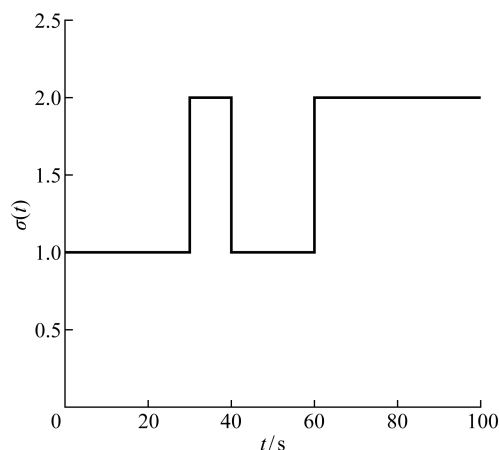


图4 切换信号

Fig. 4 Switching signal

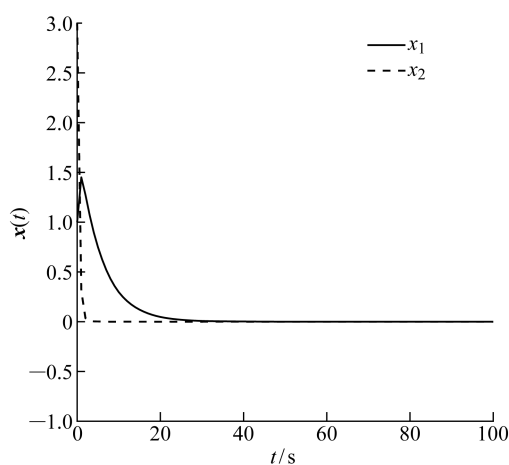


图5 系统状态轨迹

Fig. 5 System state trajectory

4 结语

切换正系统是控制理论和工程领域研究的热点问题. 针对网络化切换正系统的测量信道和控制信道同时存在周期 DoS 攻击问题, 研究了变周期切换的安全控制问题. 将攻击时长、攻击次数等相关参数转化为切换区间的长度, 得到相应系统数学模型. 利用切换方法对周期 DoS 攻击下的切换正系统进行合理建模, 设计出安全控制器保证 DoS 攻击下系统的正性及稳定性, 借助 Metzler 矩阵和多 Lyapunov 函数法从攻击周期、切换区间、切换时刻分析了系统的正性和全局渐近稳定性. 最后, 通过仿真实例验证了安全控制器的有效性.

参考文献:

[1] YAN J J, YANG G H. Switching resilient control scheme for cyber-physical systems against DoS

attacks[J]. **Journal of the Franklin Institute**, 2021, 358(8): 4257-4276.

[2] DING D, TANG Z, WANG Y, *et al.* Secure synchronization of complex networks under deception attacks against vulnerable nodes[J]. **Applied Mathematics and Computation**, 2021, 399: 126017.

[3] 王志文, 刘伟. 拒绝服务攻击下信息物理系统事件触发广义预测控制[J]. **上海交通大学学报**, 2020, 54(9): 910-915.

WANG Zhiwen, LIU Wei. Event-triggered generalized predictive control of cyber-physical systems under denial-of-service attacks[J]. **Journal of Shanghai Jiao Tong University**, 2020, 54(9): 910-915.

[4] YANG F, GU Z, TIAN E G, *et al.* Event-based switching control for networked switched systems under nonperiodic DoS jamming attacks[J]. **IET Control Theory & Applications**, 2020, 14(19): 3097-3106.

[5] ZHU Y Z, ZHENG W X. Observer-based control for cyber-physical systems with periodic DoS attacks via a cyclic switching strategy[J]. **IEEE Transactions on Automatic Control**, 2020, 65(8): 3714-3721.

[6] XING M P, LU J Q, QIU J L, *et al.* Synchronization of complex dynamical networks subject to DoS attacks: An improved coding-decoding protocol[J]. **IEEE Transactions on Cybernetics**, 2023, 53(1): 102-113.

[7] WANG P B, REN X M, ZHENG D D. Event-triggered resilient control for cyber-physical systems under periodic DoS jamming attacks[J]. **Information Sciences**, 2021, 577: 541-556.

[8] YE D, SONG Y B. Optimal periodic DoS attack with energy harvester in cyber-physical systems[J]. **Neurocomputing**, 2020, 390: 69-77.

[9] HU S L, HAN Y X, CHEN X L, *et al.* Event-triggered H_∞ filtering over wireless sensor networks under unknown periodic DoS jamming attacks[C]// **2018 Chinese Control and Decision Conference**. Shenyang, China: IEEE, 2018: 1433-1438.

[10] 宋秀兰, 俞立. 一类约束线性切换系统的滚动优化控制[J]. **上海交通大学学报**, 2015, 49(11): 1635-1640.

SONG Xiulan, YU Li. Receding optimization control for a class of constrained linear switched systems[J]. **Journal of Shanghai Jiao Tong University**, 2015, 49(11): 1635-1640.

[11] REN H L, ZONG G D, LI T S. Event-triggered finite-time control for networked switched linear systems with asynchronous switching[J]. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**,

- 2018, 48(11): 1874-1884.
- [12] QU H Q, ZHAO J. Stabilisation of switched linear systems under denial of service[J]. **IET Control Theory & Applications**, 2020, 14(11): 1438-1444.
- [13] HAN Y C, LIAN J, HUANG X. Event-triggered H^∞ control of networked switched systems subject to denial-of-service attacks[J]. **Nonlinear Analysis: Hybrid Systems**, 2020, 38: 100930.
- [14] LIU J, YANG Y K, LI H C, *et al.* Stabilisation for switched positive systems under extended asynchronous switching[J]. **IET Control Theory & Applications**, 2019, 13(16): 2702-2709.
- [15] HU J J, LIU D X, XIA D B, *et al.* Robust stabilization of switched positive discrete-time systems with asynchronous switching and input saturation[J]. **Optimal Control Applications and Methods**, 2019, 40(1): 105-118.
- [16] OGURA M, PRECIADO V M. Stability of spreading processes over time-varying large-scale networks[J]. **IEEE Transactions on Network Science and Engineering**, 2016, 3(1): 44-57.
- [17] SON J H, AHN H S. Formation coordination for the propagation of a group of mobile agents via self-mobile localization[J]. **IEEE Systems Journal**, 2015, 9(4): 1285-1298.
- [18] RAMI M A, TADEO F. Controller synthesis for positive linear systems with bounded controls[J]. **IEEE Transactions on Circuits and Systems II: Express Briefs**, 2007, 54(2): 151-155.
- [19] KUZMANOVIC A, KNIGHTLY E W. Low-rate TCP-targeted denial of service attacks and counter strategies[J]. **IEEE/ACM Transactions on Networking**, 2006, 14(4): 683-696.

(本文编辑:李博文)