控制与决策
Control and Decision

非周期性 DoS 攻击下布尔控制网络的镇定控制

白博文, 王金环

引用本文:
白博文, 王金环. 非周期性 DoS 攻击下布尔控制网络的镇定控制[J]. 控制与决策, 2025, 40(7): 2168-2174.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2024.1268

您可能感兴趣的其他文章

Articles you may be interested in

布尔控制网络的集成集可控

Ensemble set controllability of Boolean control networks

控制与决策. 2021, 36(9): 2187-2194 https://doi.org/10.13195/j.kzyjc.2019.1837

基于观测器的网络化多智能体预测控制

Observer-based networked multi-agent predictive control

控制与决策. 2021, 36(9): 2290-2296 https://doi.org/10.13195/j.kzyjc.2019.1801

基于移动传感器/执行器网络的时滞分布参数系统镇定控制

Stabilization control for a class of distributed parameter systems with time-delay based on mobile sensor and actuator networks

控制与决策. 2021, 36(8): 1955-1962 https://doi.org/10.13195/j.kzyjc.2019.1309

基于神经网络的电力系统暂态稳定分布式自适应控制

Neural network-based distributed adaptive control for power system transient stability

控制与决策. 2021, 36(6): 1407-1414 https://doi.org/10.13195/j.kzyjc.2019.1168

基于T-S模糊模型的多时滞非线性网络切换控制系统非脆弱H_∞控制

Non-fragile H_∞ control for multi-delay nonlinear network switching control system based on T-S model

控制与决策. 2021, 36(5): 1087-1094 https://doi.org/10.13195/j.kzyjc.2019.1098

非周期性 DoS 攻击下布尔控制网络的镇定控制

白博文，王金环†

(河北工业大学 理学院，天津 300401)

摘　要: 针对布尔控制网络在非周期性拒绝服务 (DoS) 攻击下的镇定控制问题, 研究服从独立同分布过程的非周期性 DoS 攻击. 首先, 将遭受攻击的布尔控制网络转化为概率布尔网络, 进而得到系统能够全局随机稳定的充分必要条件; 其次, 基于可达集构造方法, 设计能够保证系统稳定的状态反馈控制器; 最后, 通过仿真实验验证所提出理论与控制方法的有效性.

关键词: 矩阵半张量积；布尔控制网络；非周期性 DoS 攻击；独立同分布过程；状态反馈控制；镇定控制

中图分类号: TP273　　**文献标志码:** A

DOI: 10.13195/j.kzyjc.2024.1268

引用格式: 白博文, 王金环. 非周期性 DoS 攻击下布尔控制网络的镇定控制 [J]. 控制与决策, 2025, 40(7): 2168-2174.

Stabilization of Boolean control networks under aperiodic DoS attacks

BAI Bo-wen，*WANG Jin-huan*†

(School of Science，Hebei University of Technology，Tianjin 300401，China)

Abstract: This paper studies the stabilization of Boolean control networks (BCNs) under aperiodic DoS attacks. DoS attacks are a common and destructive network attack that weaken the performance of a system by blocking the transmission of information between network nodes. We focus on analyzing aperiodic DoS attacks that obey an independent and identically distributed process. First, for aperiodic DoS attacks following an independent and identically distributed process, we obtain a necessary and sufficient condition for the system stabilization by transforming the attacked BCN into a probabilistic Boolean network. Then, the state feedback control is designed using the reachable set method to ensure the system stabilization. Finally, the effectiveness of the proposed theory and control method is illustrated by a simulation example.

Keywords: semi-tensor product； Boolean control networks； aperiodic DoS attacks； independent and identically distributed process；state feedback control；stabilization

0　引　言

布尔网络是用于模拟和分析基因调控网络和细胞网络的数学模型, 自 Kauffman[1] 于 1969 年提出以来, 由于其结构的简洁性, 布尔网络迅速受到广泛关注. 在布尔网络中, 节点 (或基因) 的状态由二进制变量表示: 1 (激活) 或 0 (不激活); 节点之间的相互作用由布尔函数描述. 通过这种方式, 布尔网络能够有效地描述复杂的生物系统. 随着研究的深入, 外部控制输入被引入到布尔网络中, 形成了布尔控制网络. 然而, 由于缺乏系统且有效的分析工具, 相关研究主要针对特殊系统, 缺乏普适性. 直到 Cheng 等[2] 提出矩阵半张量积方法后, 该研究有了显著改善. 矩阵半张量积方法的优势在于能够将布尔 (控制) 网络的动力学转化为线性 (或双线性) 离散时间系统, 从而可以利用经典控制理论进行分析. 因此, 布尔 (控制) 网络得到了多方面发展, 在可控性[3]、可观性[4]、稳定性[5-6] 等关键问题上得到了广泛研究. 此外, 矩阵半张量积方法还被应用于很多领域, 例如智能电网[7]、有限自动机[8] 和有限博弈[9] 等.

镇定控制是系统理论的一个核心研究问题, 为了实现布尔控制网络的镇定控制, 设计合适的控制器至关重要. 目前, 关于布尔控制网络的镇定控制设计方法有很多, 包括状态反馈控制[10]、输出反馈控制[11]、采样数据反馈控制[12] 和牵制控制[13] 等. 其中, 状态

收稿日期: 2024-10-30；**录用日期:** 2025-01-04.
基金项目: 河北省自然科学基金项目 (F2021202032).
责任编委: 冯俊娥.
†通信作者. E-mail: jinhuan@hebut.edu.cn.

反馈控制的应用最为广泛, 并且有利于提升系统的性能, 本文将设计状态反馈控制器镇定系统.

随着信息技术的发展, 网络安全面临巨大的挑战. 影响网络安全的主要因素之一是恶意网络攻击, 其目的是窃取信息并破坏系统功能. 网络攻击的种类和复杂性不断增加, 其攻击形式大致可以分为两类: DoS 攻击[14–17] 和欺骗攻击, 欺骗攻击包括虚假数据注入攻击[18] 和重放攻击[19]. 如文献 [20] 所述, DoS 攻击比欺骗攻击需要更少的先验知识, 因此 DoS 攻击更容易实施. 大量工作揭示了恶意 DoS 攻击对控制系统的影响, 其中涉及信息物理系统[14]、多智能体系统[16] 和网络化系统[17] 等领域. 另外还有关于网络故障的研究[21-22]. 文献 [21] 通过构建故障触发和识别矩阵, 探讨了如何识别布尔网络中的去边故障. Li 等[22] 通过研究软硬两种故障攻击, 验证了移位寄存器对故障攻击的恢复能力. 但是, 布尔控制网络中关于恶意网络攻击的研究还很少[23].

DoS 攻击可分为周期性和非周期性两类. 不同于周期性 DoS 攻击, 非周期性 DoS 攻击没有固定攻击时刻, 其攻击模式更具随机性和不可预测性, 因此它的防御难度更大, 理论分析也更加复杂. Zhang 等[15] 研究了非周期离散 DoS 攻击下马尔可夫跳变系统的安全异步控制. Wu 等[17] 设计了一种基于采样数据的状态反馈安全控制器, 以提高随机 DoS 攻击下网络化控制系统的稳定性.

由于信息传输信道的固有脆弱性, 布尔控制网络极易受到各种类型的干扰和攻击. 以基因节点间的信息交互过程为例, 若系统受到外部输入有害物质的影响, 例如病毒或者药物等, 可能导致基因节点之间信息交互中断, 所以研究非周期性 DoS 攻击问题对系统安全有一定帮助. 针对布尔控制网络攻击和干扰问题, 已展开一些研究工作, 例如布尔控制网络在移动攻击下的安全性[23] 和布尔控制网络的干扰解耦[24]. 然而, 现有研究还未考虑布尔控制网络在 DoS 攻击下的镇定控制问题. 虽然传统控制系统针对 DoS 攻击的相关研究有很多[14–17], 但由于布尔控制网络是有限值逻辑系统, 传统控制系统的研究方法不能直接应用于布尔控制网络, 需要探索新的方法.

基于上述考虑, 本文研究布尔控制网络在非周期性 DoS 攻击下的镇定控制. 主要贡献如下: 1) 研究了布尔控制网络遭受非周期性 DoS 攻击时的镇定控制问题, 考虑非周期性 DoS 攻击的随机形式为独立同分布过程; 2) 针对遵循独立同分布过程的非周期性 DoS 攻击, 巧妙地将受到攻击的系统转化为一类特殊的概率布尔网络, 并得到系统全局随机镇定的充要条件; 3) 针对布尔控制网络在该攻击下如何镇定到不动点的问题, 通过构造可达集设计状态反馈控制器, 以确保系统全局随机镇定.

1　预备知识

首先给出一些本文用到的符号: $\mathcal{M}_{m\times n}$表示所有$m\times n$ 的实矩阵集合, $\Upsilon_{m\times n}$表示所有$m\times n$的概率矩阵集合; $[m:n]=\{m,m+1,\dots,n\}$, $[m:n)=\{m,m+1,\dots,n-1\}$, $(m:n)=\{m+1,m+2,\dots,n-1\}$; $\mathcal{D}:=\{0,1\}$; $\Delta_n:=\{\delta_n^i|i\in[1:n]\}$, 其中$\delta_n^i$是$I_n$的第 i 列; 矩阵 $A=[\delta_m^{i_1},\delta_m^{i_2},\dots,\delta_m^{i_n}]\triangleq\delta_m[i_1,i_2,\dots,i_n]$称为逻辑矩阵; $\mathcal{L}_{m\times n}$表示所有$m\times n$维逻辑矩阵的集合; 矩阵$\Phi_n=\delta_{2^{2n}}[1,2^n+2,2\cdot 2^n+3,\dots,(2^n-2)\cdot 2^n+2^n-1,2^{2n}]\in\mathcal{L}_{2^{2n}\times 2^n}$称为降幂矩阵, 满足$x^2=\Phi_n x$; $mn\times mn$维矩阵$W_{[m,n]}=[\delta_n^1\delta_m^1,\dots,\delta_n^n\delta_m^1,\delta_n^1\delta_m^2,\dots,\delta_n^n\delta_m^2,\dots,\delta_n^n\delta_m^n]$称为交换矩阵, 满足$W_{[m,n]}XY=YX$, 其中$X\in\mathbb{R}^m$, $Y\in\mathbb{R}^n$. 当 $m=n$时, $W_{[m,n]}$可表示为$W_{[m]}$.

下面介绍矩阵半张量积的概念, 详细信息见文献 [2].

定义 1[2]　设$A\in\mathcal{M}_{m\times n}$, $B\in\mathcal{M}_{p\times q}$, 矩阵$A$和$B$的半张量积 (STP) 定义为

$$A\ltimes B:=(A\otimes I_{\alpha/n})(B\otimes I_{\alpha/p})\in\mathcal{M}_{m\alpha/n\times q\alpha/p}.$$

其中: $\alpha=\mathrm{lcm}\{n,p\}$表示$n$和$p$的最小公倍数, $\otimes$表示 Kronecker 积.

当 $n=p$ 时, 矩阵的半张量积退化为常规的矩阵乘积. 为简化表示, 本文的半张量积省略符号“$\ltimes$”.

将逻辑值1、0分别等价于δ_2^1、δ_2^2, 则$\mathcal{D}\sim\Delta_2$. 有如下引理.

引理 1[2]　设$f:\mathcal{D}^n\to\mathcal{D}$是一个$n$元逻辑函数, 则存在唯一的$M_f\in\mathcal{L}_{2\times 2^n}$, 使得在向量形式下

$$f(x_1,x_2,\dots,x_n)=M_f\ltimes_{i=1}^n x_i,$$

其中M_f是f的结构矩阵.

2　问题描述

非周期性 DoS 攻击是一种随机攻击, 其中攻击时刻和连续攻击次数是未知的. 本文考虑非周期性 DoS 攻击遵循独立同分布的随机方式.

由于连续 DoS 攻击的次数是有界的, 假设连续攻击的最大次数为N. 集合$[0:N]$表示连续攻击次数的可能取值. 令$h_k:=t_{k+1}-t_k$, 其中$t_k(k\in\mathbb{N})$是没有攻击发生的时刻, 即休眠时刻. 显然$h_k\in[1:N+1]$, 连续攻击的次数为h_k-1. 当$h_k=1$时, 表

示在$[t_k:t_{k+1}]$内没有攻击.

注 1 能量约束是所有类型攻击者固有的限制. 由于能量的限制, 攻击者会持续消耗能量直至耗尽. 在这种情况下, 可以认为连续 DoS 攻击的次数有界.

当非周期性 DoS 攻击遵循独立同分布过程时, 假设$h_k=i$的概率为p_i, 即 DoS 攻击连续攻击$i-1$次的概率为 p_i, 从而对于$i\in[1:N+1]$有$P(h_k=i)=p_i$, 且$\sum\limits_{i=1}^{N+1}p_i=1$. 显然, 当$h_k=1$时, 表示时刻$[t_k:t_{k+1}]$没有受到 DoS 攻击; 当$h_k>1$时, 在$(t_k:t_{k+1})$内的时刻受到 DoS 攻击.

非周期性 DoS 攻击随机阻断传输通道, 导致数据丢失. 非周期性 DoS 攻击信号表示如下:

$$S_{\rm ADoS}(t)=\begin{cases}0,\ t=t_k;\\ 1,\ t\neq t_k.\end{cases}$$

其中$t_k(k\in N)$是休眠时刻.

带有攻击的布尔控制网络控制器形式如下:

$$u(t)=(1-S_{\rm ADoS}(t))u(t)+S_{\rm ADoS}(t)u(t-1).$$

图 1 展示了一个非周期性 DoS 攻击, 其中闪电符号表示 DoS 攻击, $t_k(k\in\mathbb{N})$是休眠时刻.

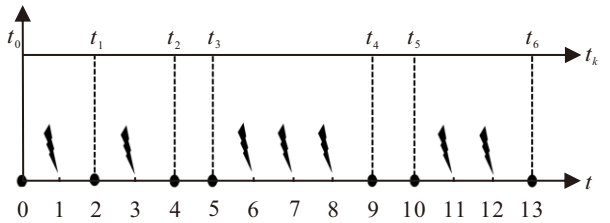

图1 非周期性 DoS 攻击示例

本文研究包含 n 个节点的布尔控制网络受到非周期性 DoS 攻击的情形. 假设非周期性 DoS 攻击发生在状态-控制信道, 将导致传输信道中的状态信息滞后. 考虑如下布尔控制网络:

$$\begin{cases}x_1(t+1)=\\ f_1(x_1(t),\dots,x_n(t),u_1(t),\dots,u_m(t)),\\ x_2(t+1)=\\ f_2(x_1(t),\dots,x_n(t),u_1(t),\dots,u_m(t)),\\ \quad\vdots\\ x_n(t+1)=\\ f_n(x_1(t),\dots,x_n(t),u_1(t),\dots,u_m(t)),\end{cases}\tag{1}$$

以及受到 DoS 攻击之后的控制器

$$\begin{aligned}&u_j(t)=e_j(x_1(t_k),\dots,x_n(t_k)),\\ &j\in[1:m],\ t\in[t_k:t_{k+1}).\end{aligned}\tag{2}$$

其中: $x_i(t)\in\mathcal{D}\,(i\in[1:n])$和$u_j(t)\in\mathcal{D}\,(j\in[1:m])$分别是$t$时刻的状态和控制输入; 映射$f_i:\mathcal{D}^{n+m}\to\mathcal{D}$和$e_j:\mathcal{D}^n\to\mathcal{D}$是逻辑函数. 假设$t_0=0$, 即初始时刻没有发生攻击.

根据引理 1, 逻辑函数f_i和e_j分别有唯一的结构矩阵L_i、K_j与之对应. 向量形式下, 令$x(t)=\ltimes_{i=1}^{n}x_i(t)\in\Delta_{2^n}$, $u(t)=\ltimes_{j=1}^{m}u_j(t)\in\Delta_{2^m}$, 则布尔控制网络 (1) 和控制器 (2) 的代数形式如下:

$$x(t+1)=Lu(t)x(t),\tag{3}$$

$$u(t)=Kx(t_k),\ t_k\leqslant t<t_{k+1}.\tag{4}$$

其中: $L=L_1*L_2*\dots*L_n\in\mathcal{L}_{2^n\times2^{n+m}}$, $K=K_1*K_2*\dots*K_m\in\mathcal{L}_{2^m\times2^n}$, "$*$" 是 Khatri-Rao 积.

如图 2 所示, 发生在状态-控制信道上的 DoS 攻击会导致控制中的状态信息滞后.

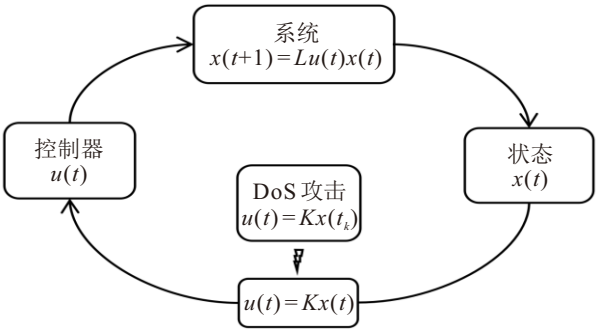

图2 DoS 攻击发生在状态-控制信道

3 主要结果

本部分首先分析布尔控制网络 (3) 在服从独立同分布的非周期性 DoS 攻击下的稳定性, 其次通过构造可达集设计相应状态反馈控制器镇定系统.

3.1 稳定性分析

假设非周期性 DoS 攻击信号遵循独立同分布过程, 即 $P(h_k=i)=p_i$, 其中 $i\in[1:N+1]$, 且$\sum\limits_{i=1}^{N+1}p_i=1$.

由布尔控制网络 (3) 和控制器 (4), 可得

$$\begin{cases}x(t_k+1)=LKx(t_k)x(t_k)=LKW_{[2^n]}\Phi_nx(t_k),\\ x(t_k+2)=(LKW_{[2^n]})^2\Phi_n^2x(t_k),\\ \quad\vdots\\ x(t_{k+1})=(LKW_{[2^n]})^{h_k}\Phi_n^{h_k}x(t_k),\end{cases}\tag{5}$$

其中 $h_k=t_{k+1}-t_k\in[1:N+1]$.

由于 $P(h_k=i)=p_i$, $i\in[1:N+1]$, 系统 (5) 可以转换为如下概率布尔网络:

$$x(t_{k+1})=\Gamma x(t_k),\tag{6}$$

其中$\Gamma\in\mathcal{L}_{2^n\times2^n}$从集合$\{\Gamma_i=(LKW_{[2^n]})^i\Phi_n^i,i\in[1:N+1]\}$中选取, 且$P(\Gamma=\Gamma_i)=p_i$, $\sum\limits_{i=1}^{N+1}p_i=1$.

令$\Pi=\sum\limits_{i=1}^{N+1}p_i\Gamma_i\in\Upsilon_{2^n\times2^n}$, 则$x(t_{k+1})$的期望为

$$\mathbb{E}\{x(t_{k+1})\} = \Pi\mathbb{E}\{x(t_k)\}. \tag{7}$$

系统 (7) 以 x_0 为初始状态的轨线记为 $x(t;x_0)$.

定义 2　如果存在一个状态$x_e \in \Delta_{2^n}$满足

$$P(x(1;x_e) = x_e) = 1,$$

则称状态x_e为一个不动点.

注 2　如果系统在任意初始状态下稳定到x_e, 则利用坐标变换[2], 系统能够全局稳定到任意状态 $x \in \Delta_{2^n}$. 不失一般性, 本文考虑系统全局稳定到 $\delta_{2^n}^{2^n}$.

类似文献 [12] 中的定义 3, 给出系统全局随机稳定的定义如下.

定义 3　给定一个不动点$\delta_{2^n}^{2^n}$. 如果对于任意初始状态$x_0 \in \Delta_{2^n}$, 均满足

$$\lim_{t\to\infty}\mathbb{E}\{x(t;x_0)\} = \delta_{2^n}^{2^n},$$

则称系统 (7) 在非周期性 DoS 攻击下$\delta_{2^n}^{2^n}$-全局随机稳定.

定义 4[25]　设 $A \in \mathbb{R}^{n\times n}$, $x(l) \in \mathbb{R}^n$. 考虑一个离散时间线性系统$x(l+1) = Ax(l)$, $l \in \mathbb{N}$. 如果矩阵 A的所有特征值的模均小于 1, 即谱半径$\rho(A) < 1$, 则A被称为 Schur 稳定的.

接下来, 给出一个在非周期性 DoS 攻击下系统 (7) 实现全局随机镇定的充分必要条件.

定理 1　系统 (7) 在非周期性 DoS 攻击下通过控制 (4) 能够全局随机镇定到$\delta_{2^n}^{2^n}$, 当且仅当满足:

1) $[LKW_{[2^n]}\Phi_n]_{2^n,2^n} = 1$;

2) 存在一个整数$1 \leqslant l \leqslant 2^n - 1$, 使得$\mathrm{Row}_{2^n}[\Pi^l] > 0$, 即对于任意的$x_0 \in \Delta_{2^n}$, 存在一条长度为$l$的可行路到达$\delta_{2^n}^{2^n}$.

证明　首先证明条件 1). 若$[LKW_{[2^n]}\Phi_n]_{2^n,2^n} = 1$成立, 则对于任意$i \in [1:N+1]$, 有$[(LKW_{[2^n]})^i\cdot(\Phi_n)^i]_{2^n,2^n} = 1$. 记$x(t_k) = \delta_{2^n}^{2^n}$. 利用数学归纳法, 已知 $[LKW_{[2^n]}\Phi_n]_{2^n,2^n} = 1$, 则 $x(t_k+1) = LKW_{[2^n]}\cdot\Phi_n\delta_{2^n}^{2^n} = \delta_{2^n}^{2^n}$成立. 假设$[(LKW_{[2^n]})^i(\Phi_n)^i]_{2^n,2^n} = 1$, $i \in [2:N]$, 即 $x(t_k+i) = (LKW_{[2^n]})^i(\Phi_n)^i\delta_{2^n}^{2^n} = \delta_{2^n}^{2^n}$. 然后得到

$$\begin{aligned} x(t_k+i+1) &= (LKW_{[2^n]})^{i+1}(\Phi_n)^{i+1}\delta_{2^n}^{2^n} = \\ &LKW_{[2^n]}x(t_k+i)\delta_{2^n}^{2^n} = \\ &LKW_{[2^n]}\Phi_n\delta_{2^n}^{2^n} = \delta_{2^n}^{2^n}, \end{aligned}$$

即$[(LKW_{[2^n]})^{i+1}(\Phi_n)^{i+1}]_{2^n,2^n} = 1$. 因此, 对于任意 $i \in [1:N+1]$都满足$[(LKW_{[2^n]})^i(\Phi_n)^i]_{2^n,2^n} = 1$.

由于系统是时不变的, 对于任意初始状态 $x_0 \in \Delta_{2^n}$, 系统的状态轨线$x(t_k;x_0)$是一条齐次马尔可夫链. 系统状态的一步转移概率矩阵为Π, 其中 $\pi_{ij} := [\Pi]_{i,j} = P(x(t_{k+1}) = \delta_{2^n}^i | x(t_k) = \delta_{2^n}^j)$. 定义 $x(t_k)$的l步转移概率矩阵为$\Pi(l)$, 即$\Pi(l) = \Pi^l$. 显然, 当且仅当$[\Pi(l)]_{i,j} > 0$时, 存在从$\delta_{2^n}^j$到$\delta_{2^n}^i$长度为l的可行路径.

对于任意初始状态$x_0 = \delta_{2^n}^j$, 有 $P(x(l;\delta_{2^n}^j) = \delta_{2^n}^{2^n}) = [\Pi(l)]_{2^n,j}$. 因此, 非周期性 DoS 攻击下的系统 (7) 能够全局随机镇定到$\delta_{2^n}^{2^n}$, 当且仅当满足

$$\Pi_\infty := \lim_{l\to\infty}\Pi(l) = \begin{bmatrix} 0_{(2^n-1)\times 2^n} \\ 1_{2^n}^{\mathrm{T}} \end{bmatrix}. \tag{8}$$

必要性. 假设在非周期性 DoS 攻击下, 系统 (7) 能够全局随机镇定到$\delta_{2^n}^{2^n}$. 对于任意$x_0 \in \Delta_{2^n}$, 可知

$$\begin{aligned} 1 = \lim_{k\to\infty}P(x(t_k) = \delta_{2^n}^{2^n} | x(0) = x_0) = \\ \lim_{k\to\infty}(P(x(t_k-1;x_0) = \delta_{2^n}^{2^n})\cdot \\ P(x(1;x(t_k-1) = \delta_{2^n}^{2^n}) = \delta_{2^n}^{2^n}) + \\ \sum_{j\neq 2^n}P(x(t_k-1;x_0) = \delta_{2^n}^j)\cdot \\ P(x(1;x(t_k-1) = \delta_{2^n}^j) = \delta_{2^n}^{2^n})) = \\ \lim_{k\to\infty}P(x(t_k-1;x_0) = \delta_{2^n}^{2^n})\cdot \\ P(x(1;x(t_k-1) = \delta_{2^n}^{2^n}) = \delta_{2^n}^{2^n}) = \\ P(x(1;\delta_{2^n}^{2^n}) = \delta_{2^n}^{2^n}). \end{aligned}$$

由于 $P(x(1;\delta_{2^n}^{2^n}) = \delta_{2^n}^{2^n}) = 1$, $\delta_{2^n}^{2^n}$是不动点. 因此$[LKW_{[2^n]}\Phi_n]_{2^n,2^n} = 1$, 即条件 1) 成立.

接下来证明条件 2). 假设在非周期性 DoS 攻击下, 系统 (7) 能够全局随机镇定到 $\delta_{2^n}^{2^n}$, 那么式 (8) 成立. 因此, 对于任意初始状态$x_0 = \delta_{2^n}^j$, 存在一条到$\delta_{2^n}^{2^n}$的可行路径. 显然, 这条可行路径的长度为$l \leqslant 2^n - 1$, 即$[\Pi(l)]_{2^n,j} > 0$, 条件 2) 成立.

充分性. 由$[LKW_{[2^n]}\Phi_n]_{2^n,2^n} = 1$可知对于任意 $i \in [1:N+1]$满足 $[(LKW_{[2^n]})^i(\Phi_n)^i]_{2^n,2^n} = 1$, 即 $[\Pi]_{2^n,2^n} = 1$. 然后, 对于任意$l \in \mathbb{N}_+$, 将矩阵$\Pi(l)$分为 4 部分, 如下所示:

$$\Pi(l) = \begin{bmatrix} \Psi^{\mathrm{T}}(l) & 0_{(2^n-1)\times 1} \\ \eta^{\mathrm{T}}(l) & 1 \end{bmatrix}. \tag{9}$$

因为$\Pi(l+1) = \Pi\times\Pi(l)$, 从而得到$\eta(l+1) = \eta(l) + \Psi(l)\eta(1)$, 可见向量$\eta(l)$是单调不减的. 根据单调有界定理, 必然存在一个向量$\mu \leqslant 1_{(2^n-1)\times 1}$使得 $\lim_{l\to\infty}\eta(l) = \mu$. 因为矩阵$\Pi(l)$每列元素之和为 1, 所以需要证明$\mu = 1_{(2^n-1)\times 1}$以确保式 (8) 成立. 等价地, 只需要证明序列$\{\eta(l)\}$的子序列$\{\eta(2^n l)\}$收敛到$1_{(2^n-1)\times 1}$即可.

由条件 2), 对于任意初始状态$\delta_{2^n}^i$ ($i \in [1:2^n]$), 存在长度为$l_i \leqslant 2^n$的可行路径到达$\delta_{2^n}^{2^n}$, 即$[\Pi(l_i)]_{2^n,i}$

>0. 然后, 记 $\iota_i:=[\Pi(l_i)]_{2^n,i}$, 可知 $[\Pi(l)]_{2^n,i}\geqslant\iota_i>0$, $\forall\, l\geqslant l_i$. 从而 $[\eta(2^n)]_i=[\Pi(2^n)]_{2^n,i}>0$, 即矩阵 $\Psi^{\rm T}(2^n)$ 的每列元素之和小于 1. 显然, 此矩阵的 1-范数 $\|\Psi^{\rm T}(2^n)\|_1<1$, 根据 $\rho(\Psi^{\rm T}(2^n))\leqslant\|\Psi^{\rm T}(2^n)\|_1<1$ 可得 $\Psi(2^n)$ Schur 稳定.

令 $\Pi(2^n(l+1))=\Pi(2^nl)\Pi(2^n)$, 则 $\eta(2^n(l+1))=\Psi(2^n)\eta(2^nl)+\eta(2^n)$. 定义 $\varphi(l)=\eta(2^nl)-1_{(2^n-1)\times1}$.

$$\begin{aligned}\varphi(l+1)=&\eta(2^n(l+1))-1_{(2^n-1)\times1}=\\&\Psi(2^n)\eta(2^nl)+\eta(2^n)-1_{(2^n-1)\times1}=\\&\Psi(2^n)(\eta(2^nl)-1_{(2^n-1)\times1})+\\&\Psi(2^n)1_{(2^n-1)\times1}+\eta(2^n)-1_{(2^n-1)\times1}=\\&\Psi(2^n)\varphi(l)+1_{(2^n-1)\times1}-1_{(2^n-1)\times1}=\\&\Psi(2^n)\varphi(l).\end{aligned}$$

因为 $\Psi(2^n)$ Schur 稳定, 所以 $\lim\limits_{l\to\infty}\varphi(l)=0$, 即 $\lim\limits_{l\to\infty}\eta(2^nl)=1_{(2^n-1)\times1}$. 因此, 式 (8) 成立, 这意味着 $\lim\limits_{t\to\infty}\mathbb{E}\{x(t;x_0)\}=\delta_{2^n}^{2^n}$. □

3.2 控制器设计

上一节通过分析非周期性 DoS 攻击独立同分布的随机方式, 得到了受攻击系统能够全局随机镇定的充要条件. 接下来, 针对服从独立同分布过程的非周期性 DoS 攻击, 设计相应的状态反馈控制器镇定受到攻击的系统.

为方便控制器设计, 系统重新构建为如下带有控制的形式:

$$\begin{aligned}&x(t_k+1)=Lu(t_k)x(t_k),\\&x(t_k+2)=Lu(t_k)Lu(t_k)x(t_k),\\&\quad\vdots\\&x(t_{k+1})=Lu(t_k)Lu(t_k)\cdots Lu(t_k)x(t_k)=\\&\qquad(\mathrm{Blk}_i(L))^{h_k}x(t_k)=\\&\qquad[L_1^{h_k},L_2^{h_k},\cdots,L_{2^m}^{h_k}]u(t_k)x(t_k)=\\&\qquad F_{h_k}u(t_k)x(t_k).\end{aligned}\tag{10}$$

其中 $L_i^{h_k}=(\mathrm{Blk}_i(L))^{h_k}$, $i\in[1:2^m]$, $F_{h_k}=[L_1^{h_k},L_2^{h_k},\cdots,L_{2^m}^{h_k}]\in\mathcal{L}_{2^n\times2^{(n+m)}}$, $h_k\in[1:N+1]$.

令 $\Xi=\sum\limits_{i=1}^{N+1}p_iF_i$, 可以得到 $x(t_{k+1})$ 的期望为

$$\mathbb{E}\{x(t_{k+1})\}=\Xi u(t_k)\mathbb{E}\{x(t_k)\},\tag{11}$$

其中 $\Xi\in\Upsilon_{2^n\times2^{(n+m)}}$.

令 $K=\delta_{2^m}[q_1,\cdots,q_{2^n}]$, 其中 $q_j\in[1:2^m]$, $j\in[1:2^n]$. 将 Ξ 等分为 2^m 个子矩阵为 $[\mathrm{Blk}_1(\Xi),\cdots,\mathrm{Blk}_{2^m}(\Xi)]$, 其中 $\mathrm{Blk}_j(\Xi)\in\Upsilon_{2^n\times2^n}$, $j\in[1:2^m]$. 根据式 (11), 假设 $x(t_k)=\delta_{2^n}^i$, 可得 $\mathbb{E}\{x(t_{k+1})\}=\mathrm{Blk}_{q_i}(\Xi)\delta_{2^n}^i$.

记 $\Omega_0=\{\delta_{2^n}^{2^n}\}$. 定义可达集如下:

$$\begin{aligned}&\Omega_1=\\&\{\delta_{2^n}^i:\exists\, q_i;\ \text{s.t. }(\mathrm{Blk}_{q_i}(\Xi)\delta_{2^n}^i)^{\rm T}(\delta_{2^n}^{2^n})>0\}\backslash\Omega_0,\\&\quad\vdots\\&\Omega_l=\\&\Big\{\delta_{2^n}^i:\exists\, q_i;\ \text{s.t. }(\mathrm{Blk}_{q_i}(\Xi)\delta_{2^n}^i)^{\rm T}\Big(\sum_{a\in\Omega_{l-1}}a\Big)>0\Big\}\Big\backslash\\&\bigcup_{0\leqslant\iota\leqslant l-1}\Omega_\iota.\end{aligned}\tag{12}$$

定理 2 非周期性 DoS 攻击下的布尔控制网络 (11) 能够通过控制 (4) 全局随机镇定到 $\delta_{2^n}^{2^n}$, 当且仅当如下条件成立:

1) $\delta_{2^n}^{2^n}$ 是一个不动点, 即 $\delta_{2^n}^{2^n}=LK\delta_{2^n}^{2^n}\delta_{2^n}^{2^n}$;

2) 存在一个正整数 $\nu\in[1:2^n-1]$, 使得 $\bigcup\limits_{\iota=0}^{\nu}\Omega_\iota=\Delta_{2^n}$.

证明 显然, 被攻击的系统能够全局随机镇定到 $\delta_{2^n}^{2^n}$, 当且仅当

$$\lim_{k\to\infty}\Xi^k=\begin{bmatrix}0_{(2^n-1)\times2^n}\\1_{2^n}^{\rm T}\end{bmatrix}.\tag{13}$$

接下来证明式 (13) 成立, 当且仅当条件 1) 和条件 2) 成立.

必要性. 若式 (13) 成立, 则对任意 $x_0\in\Delta_{2^n}$ 有

$$\lim_{k\to\infty}P(x(t_k)=\delta_{2^n}^{2^n}|x(0)=x_0)=1.$$

由定理 1 必要性的证明可得 $[LKW_{[2^n]}\Phi_n]_{2^n,2^n}=1$, 即 $\delta_{2^n}^{2^n}=LK\delta_{2^n}^{2^n}\delta_{2^n}^{2^n}$ 成立.

根据式 (13), 对于任意初始状态 $x_0\in\Delta_{2^n}$, 存在一条到 $\delta_{2^n}^{2^n}$ 的可行路径. 显然, 这条可行路径的长度 $l\leqslant2^n-1$, 即存在一个正整数 $\nu\in[1:2^n-1]$ 使得 $\bigcup\limits_{\iota=0}^{\nu}\Omega_\iota=\Delta_{2^n}$. 必要性证明完毕.

充分性. 若条件 1) 成立, 将矩阵 Ξ 分为 4 部分:

$$\Xi=\begin{bmatrix}\Xi_{11}&0_{(2^n-1)\times1}\\\Xi_{21}&1\end{bmatrix}.$$

类似地, 将 Ξ^k 分为

$$\Xi^k=\begin{bmatrix}\Xi_{11}(k)&0_{(2^n-1)\times1}\\\Xi_{21}(k)&1\end{bmatrix},$$

其中 $\Xi_{11}(k)=(\Xi_{11})^k$.

如果条件 2) 成立, 则存在一个正整数 $\nu\in[1:2^n-1]$ 使得 $\mathrm{Row}_{2^n}(\Xi^\nu)>0$. 因为矩阵 Ξ^ν 的每一列元素之和为 1, 所以 $\Xi_{11}(\nu)$ Schur 稳定. 由于 Ξ_{11} 每一列所有元素之和小于等于 1, Ξ_{11} 的谱半径 $\rho(\Xi_{11})\leqslant1$. 若 $\rho(\Xi_{11})=1$, 则有 $\rho((\Xi_{11})^\nu)=1$. 这与 $\Xi_{11}(\nu)$ Schur 稳定矛盾, 因此 $\rho(\Xi_{11})<1$, 即 Ξ_{11} Schur 稳定. 从而 $\lim\limits_{k\to\infty}\Xi_{11}(k)=\lim\limits_{k\to\infty}(\Xi_{11})^k=0_{(2^n-1)\times(2^n-1)}$, 即

式 (13) 成立. 充分性得证.

综上所述, 非周期性 DoS 攻击下的布尔控制网络 (11) 能够通过控制 (4) 全局随机镇定到$\delta_{2^n}^{2^n}$, 当且仅当条件 1) 和条件 2) 成立. □

根据定理 2, 给出设计状态反馈控制器的算法.

算法 1　设计状态反馈矩阵K.

给定不动点$\delta_{2^n}^{2^n}$. 首先计算$\Xi \in \Upsilon_{2^n\times 2^{(n+m)}}$, 进而得到$\Omega_1, \Omega_2, \ldots, \Omega_l$. 设$K = \delta_{2^m}[q_1, \ldots, q_{2^n}]$.

step 1: 对于$\delta_{2^n}^{2^n}$, 求解$\delta_{2^n}^{2^n} = LK\delta_{2^n}^{2^n}\delta_{2^n}^{2^n}$得到$q_{2^n}$;

step 2: 对于任意$x(0) = \delta_{2^n}^{r} \neq \delta_{2^n}^{2^n}$, $r = 1, 2, \ldots, 2^n - 1$, 找到$\iota \in [1 : l]$使得$x(0) \in \Omega_\iota$, 进而根据$(\mathrm{Blk}_{q_r}(\Xi)\delta_{2^n}^{r})^{\mathrm{T}}\Big(\sum\limits_{a\in\Omega_{\iota-1}} a\Big) > 0$找到所有可能的取值$q_r$, 记$q_r \in Q_r$;

step 3: 得到$K = \delta_{2^m}[q_1, q_2, \ldots, q_{2^n}]$, 其中$q_r \in Q_r$, $r \in [1 : 2^n]$.

4　仿真实验

本节将举例演示布尔控制网络在非周期性 DoS 攻击下的镇定控制, 并设计相应的状态反馈控制器.

考虑一个由 3 个状态节点和两个控制输入组成的生物凋亡网络[6], 其动态演化过程可以简化为如下布尔控制网络:

$$\begin{cases} x_1(t+1) = \neg x_2(t) \bigwedge u_1(t), \\ x_2(t+1) = \neg x_1(t) \bigwedge (\neg x_3(t)), \\ x_3(t+1) = x_2(t) \bigvee u_1(t) \bigwedge u_2(t). \end{cases} \tag{14}$$

其中: $x_1(t)$、$x_2(t)$和$x_3(t)$分别代表 3 个状态 IAP、C3a 和 C8a; $u_1(t)$和$u_2(t)$表示两个控制输入.

利用矩阵半张量积, 系统 (14) 的代数形式为

$$x(t+1) = Lu(t)x(t).$$

其中: $x(t) = \ltimes_{i=1}^{3} x_i(t)$, $u(t) = \ltimes_{i=1}^{2} u_i(t)$, 且

$$L = \delta_8[7,3,7,3,7,4,7,4,7,8,7,8,7,8,7,8,\\ 7,3,5,1,7,4,5,2,7,8,5,6,7,8,5,6].$$

设非周期性 DoS 攻击的最大连续攻击次数为 3, 即$N = 3$. 假设攻击遵循独立同分布过程, 其相应的概率为$p_1 = 0.2$, $p_2 = 0.4$, $p_3 = 0.3$及$p_4 = 0.1$.

根据式 (10), 可得F_1、F_2、F_3和F_4, 进而通过计算$\sum\limits_{i=1}^{N+1} p_i F_i$得到$\Xi \in \Upsilon_{8\times 2^{32}}$.

考虑系统的一个不动点δ_8^7. 参考式 (12) 可达集的定义, 有$\Omega_0 = \{\delta_8^7\}$, $\Omega_1 = \{\delta_8^1, \delta_8^2, \delta_8^3, \delta_8^4, \delta_8^5, \delta_8^6, \delta_8^8\}$. 显然, $\Omega_0 \bigcup \Omega_1 = \Delta_8$, 结合定理 2 可知布尔控制网络 (14) 在非周期性 DoS 攻击下能够全局随机镇定到δ_8^7.

考虑系统另一个不动点δ_8^8, 可得$\Omega_0 = \{\delta_8^8\}$, $\Omega_1 = \{\delta_8^2, \delta_8^4, \delta_8^6\}$, $\Omega_2 = \varnothing$, $\Omega_0 \bigcup \Omega_1 \bigcup \Omega_2 \neq \Delta_8$, 即系统不能全局随机镇定到$\delta_8^8$.

接下来, 设$K = \delta_8[q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8]$. 针对不动点$\delta_8^7$, 根据算法 1 可以得到$q_7 \in [1 : 2]$; q_1, $q_3, q_5 \in [1 : 4]$; $q_2, q_4, q_6, q_8 \in \{1, 3\}$.

取$K = \delta_4[1,3,4,1,2,3,2,1]$. 根据式 (6) 得到$\Gamma_i = (LKW_{[2^n]})^i \Phi_n^i$, $i \in [1 : 4]$. 进而计算得到$[(LKW_{[2^n]})\Phi_n]_{2^n,2^n} = 1$以及

$$\Pi = \sum_{i=1}^{N+1} p_i \Gamma_i = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0.4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0.2 & 0 & 0.2 & 0 & 0 & 0 & 0.4 \\ 0 & 0 & 0 & 0 & 0 & 0.2 & 0 & 0.2 \\ 0 & 0.5 & 0.5 & 0 & 0 & 0.1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0.3 & 0.5 & 0.8 & 1 & 0.3 & 1 & 0.4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

显然, 取$l = 1$时$\mathrm{Row}_7[\Pi^l] > 0$, 即对于任意的初始状态$x_0 \in \Delta_8$, 存在一条长度为$l$的可行路到达$\delta_8^7$. 因此, 定理 1 的条件成立, 由定理 1, 系统 (14) 在非周期性 DoS 攻击下能够全局随机镇定到δ_8^7.

如图 3 所示, 对于 3 个不同的初始状态δ_8^3、δ_8^6和δ_8^8, 布尔控制网络 (14) 通过状态反馈控制$u(t) = Kx(t_k)$能够全局随机收敛到δ_8^7.

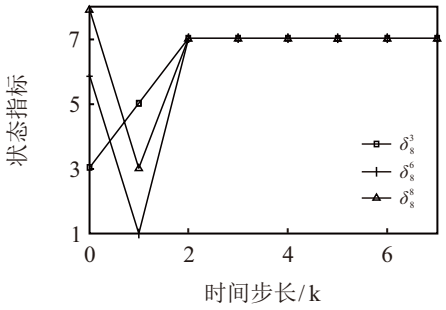

图3　系统 (14) 在初始状态 δ_8^3、δ_8^6、δ_8^8 下的轨迹

5　结　论

本文研究了遵循独立同分布过程的非周期性 DoS 攻击下布尔控制网络的镇定控制问题. 将受攻击的布尔控制网络转化为一种特殊的概率布尔网络, 并得到了概率布尔网络能够全局随机镇定的两个充要条件. 然后, 设计了相应的状态反馈控制器镇定系统. 本文的研究为非周期性 DoS 攻击下布尔控制网络的镇定控制问题提供了新的理论基础和控制方法. 进一步工作考虑布尔控制网络在其他类型网络攻击下的安全问题, 如重放攻击、错误数据注入攻击等.

参考文献 (References)

[1] Kauffman S A. Metabolic stability and epigenesis in randomly constructed genetic nets[J]. Journal of Theoretical Biology, 1969, 22(3): 437-467.

[2] Cheng D Z, Qi H S, Zhao Y. Analysis and control of Boolean networks: A semi-tensor product approach[M]. London: Springer-Verlag, 2011.

[3] Zhu Q X, Liu Y, Lu J Q, et al. Further results on the controllability of Boolean control networks[J]. IEEE Transactions on Automatic Control, 2019, 64(1): 440-442.

[4] Li Y L, Feng J E, Cheng D Z, et al. Observability decomposition of Boolean control networks under several kinds of observability[J]. IEEE Transactions on Automatic Control, 2024, 69(2): 1340-1347.

[5] Meng M, Liu L, Feng G. Stability and l_1 gain analysis of Boolean networks with Markovian jump parameters[J]. IEEE Transactions on Automatic Control, 2017, 62(8): 4222-4228.

[6] Liu J Y, Liu Y, Guo Y Q, et al. Sampled-data state-feedback stabilization of probabilistic Boolean control networks: A control Lyapunov function approach[J]. IEEE Transactions on Cybernetics, 2020, 50(9): 3928-3937.

[7] 刘敏, 王金环. 基于势博弈的智能电网需求侧管理问题[J]. 控制与决策, 2024, 39(2): 545-550.
(Liu M, Wang J H. Potential game for the demand-side management of smart grids[J]. Control and Decision, 2024, 39(2): 545-550.)

[8] Yan Y Y, Hao P L, Yue J M, et al. An STP look at logical blocking of finite state machines: Formulation, detection, and search[J]. Science China Information Sciences, 2024, 67(10): 202208.

[9] 王元华, 张秋童, 臧文科. 切换网络演化博弈的同步[J]. 控制与决策, 2024, 39(10): 3313-3318.
(Wang Y H, Zhang Q T, Zang W K. Synchronization of switched networked evolutionary games[J]. Control and Decision, 2024, 39(10): 3313-3318.)

[10] Li H T, Wang Y Z. Further results on feedback stabilization control design of Boolean control networks[J]. Automatica, 2017, 83: 303-308.

[11] Jia Y Z, Wang B, Feng J E, et al. Set stabilization of Boolean control networks via output-feedback controllers[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(12): 7527-7536.

[12] Sun L J, Ching W K. Stabilization and reconstruction of sampled-data Boolean control networks under noisy sampling interval[J]. IEEE Transactions on Automatic Control, 2023, 68(4): 2444-2451.

[13] Zhong J, Ho D W C, Lu J Q. A new approach to pinning control of Boolean networks[J]. IEEE Transactions on Control of Network Systems, 2022, 9(1): 415-426.

[14] Yan J J, Yang G H. Secure state estimation of nonlinear cyber-physical systems against DoS attacks: A multiobserver approach[J]. IEEE Transactions on Cybernetics, 2023, 53(3): 1447-1459.

[15] Zhang Y, Wu Z G. Asynchronous control of Markov jump systems under aperiodic DoS attacks[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70(2): 685-689.

[16] 路平立, 骆文城, 杜长坤. 基于动态事件驱动的多智能体系统预测控制[J]. 控制与决策, 2024, 39(12): 3981-3988.
(Lu P L, Luo W C, Du C K. Dynamic event-triggered-based predictive control of multi-agent systems[J]. Control and Decision, 2024, 39(12): 3981-3988.)

[17] Wu J, Peng C, Zhang J, et al. A sampled-data-based secure control approach for networked control systems under random DoS attacks[J]. IEEE Transactions on Cybernetics, DOI: 10.1109/TCYB.2024.3350331.

[18] 马娟, 赵海娟, 徐勤琪. 多策略虚假数据注入攻击下切换系统滑模控制的安全设计[J]. 控制与决策, 2024, 39(12): 4093-4098.
(Ma J, Zhao H J, Xu Q Q. Secure sliding mode control of switched systems under multi-strategy false data injection attacks[J]. Control and Decision, 2024, 39(12): 4093-4098.)

[19] 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.

[20] Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries[J]. Automatica, 2015, 51: 135-148.

[21] Li W R, Li H T, Yang X R. Identification of edge removal fault in Boolean networks and disjunctive Boolean networks[J]. Journal of the Franklin Institute, 2024, 361(6): 106754.

[22] Li H T, Liu Z Q, Li W R. Nonsingularity of grain-like cascade feedback shift registers subject to fault attacks[J]. Science China Information Sciences, 2024, 67: 192203.

[23] Wang L Q, Wu Z G, Lam J. Necessary and sufficient conditions for security of hidden Markov Boolean control networks under shifting attacks[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(1): 321-330.

[24] Li L L, Zhang A G, Lu J Q. Disturbance decoupling problem of delayed Boolean networks based on the network structure[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 70(3): 1004-1008.

[25] Duman A, Aydın K. Sensitivity of Schur stability of monodromy matrix[J]. Applied Mathematics and Computation, 2011, 217: 6663-6670.

作者简介

白博文 (1999−), 男, 硕士生, 主要研究方向为布尔网络建模与控制, E-mail: bbwjyy@163.com;

王金环 (1980−), 女, 教授, 博士, 主要研究方向为多智能体系统控制、博弈系统控制, E-mail: jinhuan@hebut.edu.cn.