拒绝服务攻击下的多输入多输出非线性系统无模型自适应控制

赵栩杨, 卜旭辉†, 余 威, 游东亚

(河南理工大学 电气工程与自动化学院, 河南 焦作 454000)

摘要: 针对多输入多输出(MIMO)非线性离散时间系统, 研究系统遭受拒绝服务(DoS)攻击和随机发生数据包丢失下的控制问题. 首先采用两个独立的伯努利分布对周期性DoS攻击和随机发生的数据包丢失进行建模. 其次结合DoS攻击设计无模型自适应控制(MFAC)算法, 进而通过理论分析和数学推导证明所提算法的收敛性. 并且通过结合先前时刻数据设计一种补偿算法对系统输出进行补偿, 从而抵消DoS攻击和随机丢包的影响, 减小系统超调量, 加快收敛速度使系统可以更快的达到期望输出. 最后, 通过两个仿真实例验证了算法的有效性.

关键词: 无模型自适应控制; 拒绝服务攻击; 数据丢失; MIMO非线性系统

引用格式: 赵栩杨, 卜旭辉, 余威, 等. 拒绝服务攻击下的多输入多输出非线性系统无模型自适应控制. 控制理论与应用, 2022, 39(2): 373 – 382

DOI: 10.7641/CTA.2021.10210

Model free adaptive control for multiple input and multiple output nonlinear systems under denial-of-service attacks

ZHAO Xu-yang, BU Xu-hui†, YU Wei, YOU Dong-ya

(School of Electrical Engineering and Automation, Henan Polytechnic University, Jiaozuo Henan 454000, China)

Abstract: This paper considers the control problem for multiple input and multiple output (MIMO) nonlinear discrete time systems against occurring periodic denial of service (DoS) attacks and random packet loss. Firstly, two independent Bernoulli distributions are applied to model the periodic DoS attacks and random packet loss. Then a model free adaptive control (MFAC) algorithm is designed based on the DoS attacks. Meanwhile, the convergence of the proposed algorithm is proved by theoretical analysis and mathematical derivation. Furthermore, a compensation algorithm is designed to compensate the system output by combining with the previous data to offset the impact of DoS attacks and random packet loss, reduce the system overshoot, accelerate the convergence rate, so that the system can achieve the desired output faster. Finally, the simulation results verify the effectiveness of the proposed algorithm.

Key words: model free adaptive control; DoS attacks; packet loss; MIMO nonlinear system

Citation: ZHAO Xuyang, BU Xuhui, YU Wei, et al. Model free adaptive control for multiple input and multiple output nonlinear systems under denial-of-service attacks. *Control Theory*, 2022, 39(2): 373 – 382

1 引言

近年来, 工业生产规模越来越大, 工艺过程纷繁复杂, 建立被控系统的精确模型愈发困难. 与此同时信息技术的飞速发展使得工业过程中大量的过程数据被存储, 这些数据包含了系统的基本信息, 因此如何利用这些数据设计独立于系统模型信息的控制器仍然是一个具有挑战性的问题. 无模型自适应控制是一种典型的数据驱动控制方法, 它不依赖系统的模型信息, 仅利用系统的输入输出(I/O)数据实现控制器的自适应设计[1]. 经过20多年的发展, 无模型自适应控制已经取得了丰富的理论成果[2–5], 并且在很多控制系统中得到了应用, 如快速路交通、机器人系统、智能超车系统、微电网等.

另一方面, 网络控制系统(network control system, NCS)以其传输效率高、安装灵活、数据共享等特点, 被广泛应用于智能交通、智能电网、工业过程控制等

收稿日期: 2021−03−15; 录用日期: 2021−06−23.

†通信作者. E-mail: buxuhui@gmail.com; Tel.: +86 391-3987564.

本文责任编委: 席在荣.

国家自然科学基金项目(61573130, U1804147), 河南省高校科技创新团队项目(20IRTSTHN019), 河南理工大学创新型科技团队项目(T2019–2, T2017–1), 河南省创新型科技团队项目(CXTD2016054)资助.

Supported by the National Natural Science Foundation of China (61573130, U1804147), the Innovative Scientists and Technicians Team of Henan Provincial High Education (20IRTSTHN019), the Innovative Scientists and Technicians Team of Henan Polytechnic University (T2019–2, T2017–1) and the Innovation Scientists and Technicians Troop Construction Projects of Henan Province (CXTD2016054).

诸多实际控制系统中. 但是由于网络自身的物理局限性, 在控制系统中引入网络可能会发生[6–8]: 通讯延迟、数据丢失、信道衰落、网络攻击等. 文献[9–11]分别讨论了存在通信延迟、信道衰落等无模型自适应控制问题.

需要说明的是, 网络攻击是网络控制系统中的另一个问题. 网络攻击可以分为3种主要类型[12–14]: 拒绝服务(denial of service, DoS)攻击、欺骗攻击和重放攻击. DoS攻击是最常见和最容易的攻击形式之一, 其目的是试图阻止各种物理组件之间的通信, 从而降低系统性能, 甚至使系统不稳定. 对网络攻击下的控制问题已有一些研究成果, 文献[15–16]针对单输入连续线性系统研究了周期性脉宽调制DoS攻击下的控制问题, 并设计了一种弹性控制律来更新控制器以抵抗攻击. 在此基础上, 文献[17]考虑DoS攻击下的非线性单输入单输出系统的影响, 并对系统设计弹性状态观测器. 但是实际的控制系统一般为多输入多输出(multiple input and multiple output, MIMO)系统, 因此对于MIMO系统的研究是有必要的. 对于多输入系统, 文献[18–19]考虑系统遭受周期性DoS攻击下的远程控制问题, 通过设计合理的控制算法, 并且给出系统的稳定条件和触发条件. 文献[20]中研究了DoS下的网络控制系统的H_∞控制, 设置了事件触发条件, 以节省网络资源.

以上的研究都是基于系统模型已知而建立的问题, 系统的控制取决于系统的模型信息. 而对于模型未知或难以建模的复杂控制系统网络攻击问题还没有研究. 因此, 本文主要研究周期性DoS干扰攻击下的无模型自适应控制问题. 由于网络攻击建模通常有周期性网络攻击和持续性网络攻击. 本文选择周期性DoS攻击, 从能量的角度看, 攻击者在结束攻击后进入休眠期进行能量补充, 更符合能量准则. 而且周期性DoS攻击拥有恒定的周期和占空比, 以提高攻击效率, 从而周期性DoS攻击的情况更加贴近实际.

本文的主要目的是解决MIMO非线性系统在网络环境下遭受恶意DoS攻击时的无模型自适应控制问题. 首先针对周期性DoS攻击进行建模, 结合模型设计控制算法, 并且通过结合先前时刻的数据信息设计一种补偿算法来消除DoS干扰攻击和随机丢包的影响, 使得系统可以更好更快的达到期望输出. 最后, 仿真结果验证了算法的有效性. 本文的主要贡献如下:

1) 在控制系统模型未知的情况下, 设计控制算法, 解决了存在DoS攻击时未知非线性系统的控制问题;

2) 针对DoS攻击造成的影响, 提出了补偿算法, 在保证网络控制系统稳定的前提下, 可以补偿DoS攻击对控制系统造成的影响, 加快控制系统的收敛速度;

3) 本文不仅考虑网络攻击现象, 而且还考虑了攻击者处于休眠期间控制系统由于网络带宽限制而发生的随机丢包现象, 研究更有一般意义.

2 问题描述

考虑MIMO非线性离散时间系统

$$\begin{aligned}&\boldsymbol{y}(k+1)=\\&\boldsymbol{f}(\boldsymbol{y}(k),\cdots,\boldsymbol{y}(k-n_y),\boldsymbol{u}(k),\cdots,\boldsymbol{u}(k-n_u)),\end{aligned}\tag{1}$$

其中: $\boldsymbol{u}(k)\in\mathbb{R}^m$, $\boldsymbol{y}(k)\in\mathbb{R}^m$分别是$k$时刻系统的输入和输出; n_y, n_u是两个未知的正整数, m是一个已知的整数, $\boldsymbol{f}(\cdot)\in\mathbb{R}^m$是非线性未知函数.

系统(1)满足如下两个假设:

假设 1 除有限时刻外, $\boldsymbol{f}(\cdot)$相对于控制输入$\boldsymbol{u}(k)$的偏导数是连续的.

假设 2 除有限时刻外, 控制系统(1)满足广义Lipschitz条件, 即对任意时刻k满足

$$\|\Delta\boldsymbol{y}(k+1)\|\leqslant b\|\Delta\boldsymbol{u}(k)\|,\tag{2}$$

其中: $\|\cdot\|$表示欧氏范数, $\Delta\boldsymbol{y}(k+1)=\boldsymbol{y}(k+1)-\boldsymbol{y}(k)$, $\Delta\boldsymbol{u}(k)=\boldsymbol{u}(k)-\boldsymbol{u}(k-1)$, $b>0$是一个常数.

注 1 假设1是对非线性系统设计的一种典型约束条件. 假设2是系统输出针对系统输入变化率的一种反映, 从能量的角度来看, 如果输入能量的变化是有限的, 那么输出能量的变化不可能是无限的. 许多实际的控制系统都满足此类假设, 例如液位控制系统、压力控制系统等.

基于以上两个假设, 给出了下面的定理1.

定理 1 [21] 对于满足假设1和假设2的非线性系统(1), 且对所有的k有$\|\Delta\boldsymbol{u}(k)\|\neq 0$, 一定存在一个被称为伪雅可比矩阵(pseudo Jacobi matrix, PJM)的时变参数$\boldsymbol{\Phi}(k)\in\mathbb{R}^{m\times m}$, 使得系统(1)可转化成如下数据模型:

$$\Delta\boldsymbol{y}(k+1)=\boldsymbol{\Phi}(k)\Delta\boldsymbol{u}(k),\tag{3}$$

其中系统的PJM如下所示:

$$\boldsymbol{\Phi}(k)=\begin{bmatrix}\phi_{11}(k)&\phi_{12}(k)&\cdots&\phi_{1m}(k)\\\phi_{21}(k)&\phi_{22}(k)&\cdots&\phi_{2m}(k)\\\vdots&\vdots&&\vdots\\\phi_{m1}(k)&\phi_{m2}(k)&\cdots&\phi_{mm}(k)\end{bmatrix}\in\mathbb{R}^{m\times m}.$$

假设上述MIMO非线性系统在网络环境下运行如图1所示, 传感器、控制器、执行器和保持器组成网络控制系统. 传感器与控制器之间的测量信道通过无线信道传递信息. 假设攻击者对测量信道发动DoS干扰攻击. 同时, 还考虑由网络内部因素如带宽限制和网络拥塞引起的随机数据包丢失.

2.1 DoS攻击和随机丢包建模

假设能量有限的DoS攻击者干扰传感器测量中的

通信链路, 由于能量限制, 攻击者只能在给定时间内攻击有限数量的通信信道, 此后攻击者停止攻击, 切换到休眠期补充能量, 为下一阶段攻击做准备, 更好的利用能量. 本文将上述DoS攻击视为一种周期性攻击, 该攻击可以建模为能量受限的周期性DoS干扰攻击模型. 攻击者的任意工作周期可表示为$k \in [(n-1)T, nT]$, 攻击者任意工作周期如图2所示.

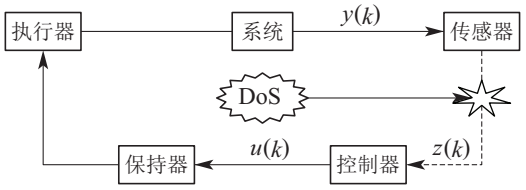

图 1 DoS干扰攻击下的网络控制系统

Fig. 1 Network control system under DoS jamming attack

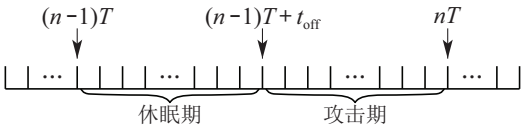

图 2 DoS干扰攻击工作周期示意图

Fig. 2 Diagram of DoS jamming attack work cycle

在图2中, T为常数, 表示攻击者任意一个工作周期的持续时间; n表示攻击者的第n个工作周期; 常数t_{off} ($t_{\text{off}} \in \mathbb{Z}^+, t_{\text{off}} \leqslant T$)表示攻击者在任意一个工作周期内的休眠期持续时间.

定义$\xi(k) \in \{1,2\}$表示攻击者处于不同时期,

$$\xi(k)=\begin{cases}1,\ k\in[(n-1)T,(n-1)T+t_{\text{off}}],\\ 2,\ k\in[(n-1)T+t_{\text{off}},nT],\end{cases} \tag{4}$$

其中: $\xi(k)=1$表示攻击者处于第n个休眠期, 干扰信号断开; $\xi(k)=2$表示攻击者处于第n个攻击期, 干扰信号通过, 通信受阻.

由于无线信道本身的特点, 如带宽限制和网络拥塞, 数据包在传输过程中会随机丢失. 假设丢包现象在休眠期仍然发生, 在数据包丢失和DoS干扰攻击下, 数据包传输的成功率应该遵循伯努利分布.

定义$\beta(k)$表示在周期性DoS干扰攻击下, k时刻的数据包是否传输成功.

$$\beta(k)=\begin{cases}1,\ \text{传输成功};\\ 0,\ \text{传输失败}.\end{cases} \tag{5}$$

在休眠期时, 定义数据传输成功的概率是$P(\beta(k)=1)=\bar{\beta}_1$, 否则$P(\beta(k)=0)=1-\bar{\beta}_1$. 在攻击期时, 定义数据传输成功的概率是$P(\beta(k)=1)=\bar{\beta}_2$, 否则$P(\beta(k)=0)=1-\bar{\beta}_2$. 综上, 可以得到

$$\begin{cases}P(\beta(k)=1)=\bar{\beta}_{\xi(k)},\\ P(\beta(k)=0)=1-\bar{\beta}_{\xi(k)},\end{cases} \tag{6}$$

其中$\bar{\beta}_{\xi(k)}$代表在休眠期或攻击期的数据传输成功概率, 故$0 \leqslant \bar{\beta}_{\xi(k)} \leqslant 1$.

注 2　在以往的研究中, 只要网络遭受攻击, 数据就传输失败, 本文考虑的是在DoS干扰攻击期间数据有传输成功的概率, 但是低于休眠期的传输成功率.

2.2　控制算法设计

在本节, 将设计一种控制算法, 在现有无模型自适应控制算法基础上, 考虑DoS干扰攻击和随机丢包的影响, 结合第2.1节对DoS干扰攻击建立的模型, 针对MIMO系统设计新的控制算法, 用于削弱周期性DoS干扰攻击的影响. 结合式(4)–(5)在DoS干扰攻击下MIMO非线性离散系统(1)可以表示为

$$\boldsymbol{y}(k)=\begin{bmatrix}\beta_{\xi(k)}(1) & & & \\ & \beta_{\xi(k)}(2) & & \\ & & \ddots & \\ & & & \beta_{\xi(k)}(m)\end{bmatrix}\begin{bmatrix}y_1(k)\\ y_2(k)\\ \vdots\\ y_m(k)\end{bmatrix}. \tag{7}$$

令$\boldsymbol{\beta}_{\xi(k)}(k)=\text{diag}\{\beta_{\xi(k)}(i)\}$, 而$\beta_{\xi(k)}(i)\in\{0,1\}$, $i=1,\cdots,m$.

假设$\text{E}(\beta_{\xi(k)}(i))=\bar{\beta}_{\xi(k)}$是已知的, 因此记$\text{E}(\boldsymbol{\beta}_{\xi(k)}(k))=\text{E}(\text{diag}\{\beta_{\xi(k)}(i)\})=\bar{\boldsymbol{\beta}}_{\xi(k)}$. 并且假设控制器可以检测出当前时刻系统在遭受DoS干扰攻击下输出信号是否传输成功.

定义

$$z_i(k)=\begin{cases}y_i(k), & \beta_{\xi(k)}(i)=1;\\ z_i(k-1), & \beta_{\xi(k)}(i)=0,\end{cases} \tag{8}$$

其中: $i=1,\cdots,m$; 且$\boldsymbol{z}(k)=[z_1(k)\ z_2(k)\cdots z_m(k)]^{\text{T}}$.

控制器无模型自适应(model free adaptive control, MFAC)算法设计如下:

$$\hat{\boldsymbol{\Phi}}(k)=\hat{\boldsymbol{\Phi}}(k-1)+\boldsymbol{\beta}_{\xi(k)}(k)\times\frac{\eta(\Delta\boldsymbol{z}(k)-\hat{\boldsymbol{\Phi}}(k-1)\Delta\boldsymbol{u}(k-1))\Delta\boldsymbol{u}^{\text{T}}(k-1)}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2}, \tag{9}$$

$$\begin{aligned}&\hat{\phi}_{ii}(k)=\hat{\phi}_{ii}(1),\\ &\text{如果}|\hat{\phi}_{ii}(k)|<b_2\text{或}|\hat{\phi}_{ii}(k)|>\alpha b_2\text{或}\\ &\text{sgn}\{\hat{\phi}_{ii}(k)\}\neq\text{sgn}\{\hat{\phi}_{ii}(1)\},\end{aligned} \tag{10}$$

$$\begin{aligned}&\hat{\phi}_{ij}(k)=\hat{\phi}_{ij}(1),\\ &\text{如果}|\hat{\phi}_{ij}(k)|>b_1\text{或}\\ &\text{sgn}\{\hat{\phi}_{ij}(k)\}\neq\text{sgn}\{\hat{\phi}_{ij}(1)\},\ i\neq j,\end{aligned} \tag{11}$$

$$\boldsymbol{u}(k)=\boldsymbol{u}(k-1)+\frac{\boldsymbol{\beta}_{\xi(k)}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}\times(\rho\hat{\boldsymbol{\Phi}}^{\text{T}}(k)(\boldsymbol{y}_d(k+1)-\boldsymbol{z}(k))), \tag{12}$$

其中: $\Delta \boldsymbol{z}(k)=\boldsymbol{z}(k)-\boldsymbol{z}(k-1)$; $|\hat{\phi}_{ij}(1)|$是$|\hat{\phi}_{ij}(k)|$的初值; $i,j=1,\cdots,m$. λ,μ是权重因子, 它们用来限制控制输入的变化保证控制输入信号具有一定平滑性, 一般情况下设置为$\lambda>0,\mu>0$. 而η,ρ代表步长, 引入它们是为了更好的保障系统稳定性, 一般设置为$\eta\in(0,2],\rho\in(0,1]$且

$$\xi(k)=\begin{cases}1,\ k\in[(n-1)T,(n-1)T+t_{\text{off}}];\\ 2,\ k\in[(n-1)T+t_{\text{off}},nT].\end{cases}$$

注 3 将λ引入控制算法(12)中, 是用来限制控制输入的变化$\Delta\boldsymbol{u}(k)$, 因此选取合适的λ可以用来保证控制输入信号具有一定的平滑性, 并能获得较好的控制性能.

3 主要结果

由于系统在随机丢包和DoS干扰攻击下会发生数据传输失败, 数据传输成功率$\beta_{\xi(k)}(k)$引入系统, 使得系统(1)转化为随机系统, 从而传统的分析方法不能适用于DoS干扰攻击和随机丢包下的控制系统稳定性分析. 因此在本节中, 在数学期望意义下对系统的稳定性进行分析. 在进行稳定性分析前先介绍以下引理和假设.

引理 1 [22] 令$A=[a_{ij}]\in\mathbb{C}^{n\times n}$, 定义盖氏圆盘如下$D_i=\{z||z-a_{ii}|\leqslant\sum\limits_{j=1,j\neq i}^{n}|a_{ii}|\}, z\in C, 1\leqslant i\leqslant n$, 则矩阵$A$的所有特征值$z_1,z_2,\cdots,z_n$都满足$z_i\in D_A=\bigcup\limits_{i=1}^{n}D_i$.

假设 3 系统的$\boldsymbol{\Phi}(k)$是满足如下条件的对角占优矩阵, 即满足$|\phi_{ji}(k)|\leqslant b_1, b_2\leqslant|\phi_{ii}(k)|\leqslant\alpha b_2, i,j=1,\cdots,m, i\neq j$, 且$\boldsymbol{\Phi}(k)$中所有元素的符号对任何时刻$k$保持不变.

注 4 假设3是对闭环数据输入输出关系的假设, 对于MIMO非线性系统, 由于系统模型未知, 仅有系统当前时刻之前的I/O数据, 系统I/O数据关系的对角占优条件可能是表示系统耦合的最终选择. 严格来说, 如果数据量足够丰富, 假设3是可以验证的.

定理 2 考虑在DoS干扰攻击和发生随机丢包下的非线性离散时间MIMO系统(1), 在假设1和假设2满足的条件下, 当$\boldsymbol{y}_d(k+1)=\boldsymbol{y}_d=\text{const}$和输出数据不完全丢失时, 存在一个正数$\lambda_{\min}>0$, 使得当$\lambda\geqslant\lambda_{\min}$时有: 系统跟踪误差序列是收敛的, 且$\lim\limits_{k\to\infty}\|\boldsymbol{y}(k+1)-\boldsymbol{y}_d\|_v=0$, 其中$\|(\cdot)\|_v$是$(\cdot)$的相容范数.

证 定理证明有两个部分, 如下所示.

1) 估计值$\hat{\boldsymbol{\Phi}}(k)$的有界性.

令$\hat{\boldsymbol{\Phi}}(k)=[\hat{\boldsymbol{\phi}}_1(k)\ \cdots\ \hat{\boldsymbol{\phi}}_m(k)]^{\mathrm{T}}$, $\hat{\boldsymbol{\phi}}_i(k)=[\hat{\phi}_{i1}(k)\ \cdots\ \hat{\phi}_{im}(k)], i=1,\cdots,m$. 参数估计算法(9)重写为

$$\hat{\boldsymbol{\phi}}_i(k)=\hat{\boldsymbol{\phi}}_i(k-1)+\frac{\eta\beta_{\xi(k)}(i)}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2}\times(\Delta z_i(k)-\hat{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}(k-1))\Delta\boldsymbol{u}^{\mathrm{T}}(k-1).\tag{13}$$

令$\tilde{\boldsymbol{\phi}}_i(k)=\hat{\boldsymbol{\phi}}_i(k)-\boldsymbol{\phi}_i(k)$, 并将式(13)两边同时减去$\boldsymbol{\phi}_i(k)$得

$$\tilde{\boldsymbol{\phi}}_i(k)=\tilde{\boldsymbol{\phi}}_i(k-1)+\boldsymbol{\phi}_i(k-1)-\boldsymbol{\phi}_i(k)+\beta_{\xi(k)}(i)\frac{\eta\tilde{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}(k-1)\Delta\boldsymbol{u}^{\mathrm{T}}(k-1)}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2}.\tag{14}$$

由定理1可知$\|\boldsymbol{\Phi}(k)\|$有上界, 即存在一个正数$\bar{b}$使得$\|\boldsymbol{\Phi}(k)\|<\bar{b}$, 因此有$\|\boldsymbol{\phi}_i(k-1)-\boldsymbol{\phi}_i(k)\|\leqslant 2\bar{b}$. 式(14)两边取范数, 并取期望可得

$$E(\|\tilde{\boldsymbol{\phi}}_i(k)\|)\leqslant 2\bar{b}+E(\|\tilde{\boldsymbol{\phi}}_i(k-1)\|)\times E(\|(1-\bar{\beta}_{\xi(k)}\frac{\eta\Delta\boldsymbol{u}(k-1)\Delta\boldsymbol{u}^{\mathrm{T}}(k-1)}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2})\|).\tag{15}$$

对式(15)右端第2项取平方, 有

$$\begin{aligned}&E(\|\tilde{\boldsymbol{\phi}}_i(k-1)(1-\bar{\beta}_{\xi(k)}\frac{\eta\Delta\boldsymbol{u}(k-1)\Delta\boldsymbol{u}^{\mathrm{T}}(k-1)}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2})\|^2)=\\&E(\|\tilde{\boldsymbol{\phi}}_i(k-1)\|^2+(-2+\bar{\beta}_{\xi(k)}\frac{\eta\|\Delta\boldsymbol{u}(k-1)\|^2}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2})\times\frac{\bar{\beta}_{\xi(k)}\eta\|\tilde{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}^{\mathrm{T}}(k-1)\|^2}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2}).\end{aligned}\tag{16}$$

对于$0<\eta\leqslant 2,\mu>0$和$\bar{\beta}_{\xi(k)}\in(0,1)$使得下式成立:

$$-2+\bar{\beta}_{\xi(k)}\frac{\eta\|\Delta\boldsymbol{u}(k-1)\|^2}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2}<0.\tag{17}$$

式(16)–(17)意味着存在$0<d_1<1$, 使得下式成立:

$$\begin{aligned}&E(\|\tilde{\boldsymbol{\phi}}_i(k)\|)\leqslant\\&E(d_1\|\tilde{\boldsymbol{\phi}}_i(k-1)\|)+2\bar{b}\leqslant\cdots\leqslant\\&d_1^kE(\|\tilde{\boldsymbol{\phi}}_i(1)\|)+\frac{2\bar{b}(1-d_1^{k-1})}{1-d_1}.\end{aligned}\tag{18}$$

式(18)意味着$\tilde{\boldsymbol{\phi}}_i(k)$是有界的, 而$\boldsymbol{\phi}_i(k)$有界, 因此可得随机丢包和DoS干扰攻击下的系统的$\hat{\boldsymbol{\phi}}_i(k)$和$\hat{\boldsymbol{\Phi}}(k)$都是有界的.

2) 跟踪误差$\boldsymbol{e}(k)$的收敛性.

定义跟踪误差:

$$\boldsymbol{e}(k)=\boldsymbol{y}_d-\boldsymbol{y}(k),\tag{19}$$

$$\boldsymbol{e}(k+1)=\boldsymbol{e}(k)-\boldsymbol{\Phi}(k)\Delta\boldsymbol{u}(k)=(\boldsymbol{I}-\boldsymbol{\beta}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2})\boldsymbol{e}(k).\tag{20}$$

参考系统与控制理论线性代数知识[23], 矩阵谱半径结论可知, 存在一个任意小的正数ε_1, 并且对式(20)两端取期望使得

$$\begin{aligned}&\mathrm{E}(\|\boldsymbol{I}-\boldsymbol{\beta}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}\|_v)<\\&\mathrm{E}(s(\boldsymbol{I}-\bar{\boldsymbol{\beta}}_{\xi(k)}\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}))+\varepsilon_1<\\&1-\rho M_1+\varepsilon_1<1,\end{aligned}\tag{21}$$

其中: $s(A)$是矩阵的谱半径, $\|A\|_v$是矩阵A的相容范数, M_1是一个大于零的正数. 令$d_2=1-\rho M_1+\varepsilon_1$. 由式(20)–(21)可得

$$\begin{aligned}&\mathrm{E}(\|\boldsymbol{e}(k+1)\|_v)\leqslant d_2\mathrm{E}(\|\boldsymbol{e}(k)\|_v)\leqslant\cdots\leqslant\\&d_2^kE(\|\boldsymbol{e}(1)\|_v).\end{aligned}\tag{22}$$

由式(22)可知$\boldsymbol{e}(k)$有界, 由定理2可知$\boldsymbol{y}_d$是给定的常向量, 因此可得$y(k)$输出的有界性. 从而可以得出MIMO–MFAC系统的有界输入输出, 至此定理2证明结束.

注 5　由定理1可知所设计的算法在DoS干扰攻击时系统还可以保持良好的稳定性, 但考虑到MIMO系统在DoS干扰攻击下并不是所有的输出结果都会传输失败, 在遭受恶意DoS干扰攻击时, 会对系统稳定性带来一定的影响, 因此设计以下的补偿算法来抵消这种负面影响.

4　补偿算法

4.1　控制器设计

由于多输入多输出系统遭受DoS干扰攻击时, 系统的输出信号不会全部传输失败, 因此设计以下的补偿算法对系统输出进行补偿:

$$\bar{y}_i(k)=\begin{cases}y_i(k),\ \beta_{\xi(k)}(i)=1;\\ \hat{y}_i(k),\ \beta_{\xi(k)}(i)=0,\end{cases}\tag{23}$$

其中: $i=1,\cdots,m,\hat{y}_i(k)$是输出$y_i(k)$的估计值. 因此, 当发生DoS干扰攻击造成输出信号传输失败时, 可以利用先前时刻数据信息$y_i(k-1)$, $\hat{\boldsymbol{\phi}}_i(k-1)$和$\Delta\boldsymbol{u}(k-1)$设计预测方程对$y_i(k)$进行补偿.

$$\hat{y}_i(k)=\bar{y}_i(k-1)+\hat{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}(k-1),\tag{24}$$

而$\bar{\boldsymbol{y}}(k)=[\bar{y}_1(k)\ \ \bar{y}_2(k)\ \ \cdots\ \ \bar{y}_m(k)]^{\mathrm{T}}$.

DoS干扰攻击下带有补偿的MFAC控制方案

$$\begin{aligned}&\hat{\boldsymbol{\Phi}}(k)=\\&\hat{\boldsymbol{\Phi}}(k-1)+\frac{\eta\boldsymbol{\beta}_{\xi(k)}(k)}{\mu+\|\Delta\boldsymbol{u}(k-1)\|^2}\times\\&(\bar{\boldsymbol{y}}(k)-\bar{\boldsymbol{y}}(k-1)-\hat{\boldsymbol{\Phi}}(k-1)\Delta\boldsymbol{u}(k-1))\times\\&\Delta\boldsymbol{u}^{\mathrm{T}}(k-1),\\&\boldsymbol{u}(k)=\\&\boldsymbol{u}(k-1)+\frac{\rho\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+|\hat{\boldsymbol{\Phi}}(k)|^2}\times(\boldsymbol{y}_d(k+1)-\bar{\boldsymbol{y}}(k)),\end{aligned}\tag{25}$$

其中

$$\xi(k)=\begin{cases}1,\ k\in[(n-1)T,(n-1)T+t_{\mathrm{off}}];\\ 2,\ k\in[(n-1)T+t_{\mathrm{off}},nT].\end{cases}$$

与算法(12)相比补偿算法(26)利用了来自先前时刻的更多信息, 采用了预测算法, 利用先前时刻的数据对其进行估计, 使控制性能预期更好.

4.2　收敛性分析

定理 3　若非线性非仿射系统(1)在遭受DoS干扰攻击时, 在假设1和假设2满足的条件下, 当$\boldsymbol{y}_d(k+1)=\boldsymbol{y}_d=\mathrm{const}$和输出数据不完全丢失时, 存在一个正数$\lambda_{\min}>0$, 使得当$\lambda\geqslant\lambda_{\min}$时, 所提出的补偿算法(25)–(26)保证:

1) 对于$\forall k,\hat{\boldsymbol{\Phi}}(k)$是有界的;

2) 系统跟踪误差是有界且收敛的.

由于在第3部分已经证明$\hat{\boldsymbol{\Phi}}(k)$的收敛性, 接下来证明误差$\boldsymbol{e}(k+1)$的收敛性.

首先考虑$\boldsymbol{y}(k)$中任意一个分量$y_i(k)$, 在DoS干扰攻击情况下, 因为在攻击期并不会所有的输出信号均传输失败, 因此假设在相邻的两个输出信号传输成功时刻k_{j-1}和k_j, $j=1,2,\cdots$.

对于DoS干扰攻击下输出数据失败时刻$k_{j-1}+1$, 根据预测方程(24)可得

$$\bar{y}_i(k_{j-1}+1)=y_i(k_{j-1})+\hat{\boldsymbol{\phi}}_i(k_{j-1})\Delta\boldsymbol{u}(k_{j-1}).\tag{27}$$

对于DoS干扰攻击下输出数据失败时刻$k_{j-1}+2$,

$$\begin{aligned}&\bar{y}_i(k_{j-1}+2)=\\&\bar{y}_i(k_{j-1}+1)+\hat{\boldsymbol{\phi}}_i(k_{j-1}+1)\Delta\boldsymbol{u}(k_{j-1}+1)=\\&y_i(k_{j-1})+\hat{\boldsymbol{\phi}}_i(k_{j-1})\Delta\boldsymbol{u}(k_{j-1})+\\&\hat{\boldsymbol{\phi}}_i(k_{j-1}+1)\Delta\boldsymbol{u}(k_{j-1}+1).\end{aligned}\tag{28}$$

依此类推, 对于DoS干扰攻击下的数据传输失败时刻k_j-1, 有

$$\begin{aligned}&\bar{y}_i(k_j-1)=\\&\bar{y}_i(k_j-2)+\hat{\boldsymbol{\phi}}_i(k_j-2)\Delta\boldsymbol{u}(k_j-2)=\\&\bar{y}_i(k_j-3)+\hat{\boldsymbol{\phi}}_i(k_j-3)\Delta\boldsymbol{u}(k_j-3)+\\&\hat{\boldsymbol{\phi}}_i(k_j-2)\Delta\boldsymbol{u}(k_j-2)=\\&\qquad\vdots\\&y_i(k_{j-1})+\hat{\boldsymbol{\phi}}_i(k_{j-1})\Delta\boldsymbol{u}(k_{j-1})+\cdots+\\&\hat{\boldsymbol{\phi}}_i(k_j-2)\Delta\boldsymbol{u}(k_j-2).\end{aligned}\tag{29}$$

综上所述, 对于DoS干扰攻击下分量$y_i(k)$输出信

号传输失败时刻$k_{j-1}<k<k_j$, 有

$$\begin{aligned}&\bar{y}_i(k)=\\&\bar{y}_i(k-1)+\hat{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}(k-1)=\\&\bar{y}_i(k-2)+\hat{\boldsymbol{\phi}}_i(k-2)\Delta\boldsymbol{u}(k-2)+\\&\hat{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}(k-1)=\\&\qquad\vdots\\&y_i(k_{j-1})+\hat{\boldsymbol{\phi}}_i(k_{j-1})\Delta\boldsymbol{u}(k_{j-1})+\cdots+\\&\hat{\boldsymbol{\phi}}_i(k_j-2)\Delta\boldsymbol{u}(k_j-2)+\\&\hat{\boldsymbol{\phi}}_i(k-1)\Delta\boldsymbol{u}(k-1),\end{aligned}\tag{30}$$

且$\bar{\boldsymbol{y}}(k)=[\bar{y}_1(k)\ \ \bar{y}_2(k)\ \ \cdots\ \ \bar{y}_m(k)]^{\mathrm{T}}$.

由式(19)可知系统跟踪误差$\boldsymbol{e}(k)=\boldsymbol{y}_d-\boldsymbol{y}(k)$.

控制算法(26)可改写为

$$\boldsymbol{u}(k)=\begin{cases}\boldsymbol{u}(k-1)+\dfrac{\rho\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)\boldsymbol{e}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2},\\ \boldsymbol{\beta}_{\xi(k)}(k)=I(k{=}k_{j-1}\text{或}k{=}k_j);\\ \boldsymbol{u}(k-1)+\dfrac{\rho\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}\times\\ (\boldsymbol{e}(k_{j-1})-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\times\\ (\hat{\boldsymbol{\Phi}}(k_{j-1})\Delta\boldsymbol{u}(k_{j-1})-\cdots-\\ \hat{\boldsymbol{\Phi}}(k-1)\Delta\boldsymbol{u}(k-1))),\\ \boldsymbol{\beta}_{\xi(k)}(k)\neq I(k_{j-1}<k<k_j).\end{cases}\tag{31}$$

对$\boldsymbol{\beta}_{\xi(k)}(k)$进行取非运算, 记做$\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)$.

令$\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)=\mathrm{diag}[\tilde{\beta}_{\xi(k)}(i)]$, 而$\tilde{\beta}_{\xi(k)}(i)\in\{0,1\}$, $i=1,\cdots,m$.

假设$\mathrm{E}(\tilde{\beta}_{\xi(k)}(i))=\bar{\tilde{\beta}}_{\xi(k)}\in(0,1)$, 因此记

$$\mathrm{E}(\tilde{\boldsymbol{\beta}}_{\xi(k)}(k))=\mathrm{E}(\mathrm{diag}\{\tilde{\beta}_{\xi(k)}(i)\})=\bar{\tilde{\boldsymbol{\beta}}}_{\xi(k)}.$$

定义$\boldsymbol{C}(k)=\boldsymbol{I}-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\dfrac{\rho\hat{\boldsymbol{\Phi}}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}$.

由式(31)可得

$$\Delta\boldsymbol{u}(k)=\frac{\rho\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)\prod\limits_{j=k_{j-1}}^{k-1}\boldsymbol{C}(j)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}\boldsymbol{e}(k_{j-1}),\tag{32}$$

其中$\boldsymbol{\beta}_{\xi(k)}(k)\neq I\ (k_{j-1}<k<k_j)$.

若$\boldsymbol{e}(k_{j-1})\neq0$, 则可知$\Delta\boldsymbol{u}(k)\neq0$, 可得

$$\begin{aligned}&\boldsymbol{y}(k)=\\&\boldsymbol{y}(k-1)+\boldsymbol{\Phi}(k-1)\Delta\boldsymbol{u}(k-1)=\\&\boldsymbol{y}(k-2)+\boldsymbol{\Phi}(k-2)\Delta\boldsymbol{u}(k-2)+\\&\boldsymbol{\Phi}(k-1)\Delta\boldsymbol{u}(k-1)=\\&\qquad\vdots\\&\boldsymbol{y}(k_{j-1})+\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\times\\&(\boldsymbol{\Phi}(k_{j-1})\Delta\boldsymbol{u}(k_{j-1})+\cdots+\\&\boldsymbol{\Phi}(k-1)\Delta\boldsymbol{u}(k-1)).\end{aligned}\tag{33}$$

将式(32)–(33)带入系统误差方程可得

$$\begin{aligned}&\boldsymbol{e}(k)=\\&\boldsymbol{e}(k_{j-1})-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\times(\boldsymbol{\Phi}(k_{j-1})\Delta\boldsymbol{u}(k_{j-1})+\cdots+\\&\boldsymbol{\Phi}(k-1)\Delta\boldsymbol{u}(k-1))=\\&\boldsymbol{e}(k_{j-1})(\boldsymbol{I}-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k))\times\\&(\frac{\rho\boldsymbol{\Phi}(k_{j-1})\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k_{j-1})}{\lambda+\|\hat{\boldsymbol{\Phi}}(k_{j-1})\|^2}+\cdots+\\&\frac{\rho\boldsymbol{\Phi}(k-2)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k-2)\prod\limits_{j=k_{j-1}}^{k-2}\boldsymbol{C}(j)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k-2)\|^2}+\\&\frac{\rho\boldsymbol{\Phi}(k-1)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k-1)\prod\limits_{j=k_{j-1}}^{k-1}\boldsymbol{C}(j)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k-1)\|^2}).\end{aligned}\tag{34}$$

由式(18)可得$\|\hat{\boldsymbol{\Phi}}(k)\|$有界, 因此存在一个正数$\bar{b}_1$使得对任意时刻$k$有$\varepsilon\leqslant\|\hat{\boldsymbol{\Phi}}(k)\|\leqslant\bar{b}_1$, 接着参考系统与控制理论线性代数知识[23], 由矩阵谱半径结论可知, 存在一个任意小的正数ε_2, 使得

$$\begin{aligned}&\mathrm{E}(\|\boldsymbol{I}-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}\|_v)\leqslant\\&\mathrm{E}(s(\boldsymbol{I}-\bar{\tilde{\boldsymbol{\beta}}}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}))+\varepsilon_2\leqslant\\&1-\rho M_2+\varepsilon_2<1,\end{aligned}\tag{35}$$

其中M_2是一个正数. 令$\bar{c}=1-\rho M_2+\varepsilon_2$, 因此$0<\boldsymbol{C}(k)<1-\rho M_2+\varepsilon_2=\bar{c}<1$.

$$\begin{aligned}&\boldsymbol{I}-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)(\frac{\rho\boldsymbol{\Phi}(k_{j-1})\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k_{j-1})}{\lambda+\|\hat{\Phi}(k_{j-1})\|^2}+\cdots+\\&\frac{\rho\boldsymbol{\Phi}(k-2)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k-2)\prod\limits_{j=k_{j-1}}^{k-2}\boldsymbol{C}(j)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k-2)\|^2}+\\&\frac{\rho\boldsymbol{\Phi}(k-1)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k-1)\prod\limits_{j=k_{j-1}}^{k-1}\boldsymbol{C}(j)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k-1)\|^2})\leqslant\\&(\boldsymbol{I}-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}\times\\&(1+\bar{c}+\cdots+\bar{c}^{k-k_{j-1}})).\end{aligned}\tag{36}$$

参照式(35)对式(36)两端取相容范数可得

$$\begin{aligned}&(\|\boldsymbol{I}-\tilde{\boldsymbol{\beta}}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}d_3\|_v)\leqslant\\&\mathrm{E}(s(\boldsymbol{I}-\bar{\tilde{\boldsymbol{\beta}}}_{\xi(k)}(k)\frac{\rho\boldsymbol{\Phi}(k)\hat{\boldsymbol{\Phi}}^{\mathrm{T}}(k)}{\lambda+\|\hat{\boldsymbol{\Phi}}(k)\|^2}d_3))+\varepsilon_3\leqslant\\&1-\rho M_3+\varepsilon_3<1,\end{aligned}\tag{37}$$

其中: $d_3=(1+\bar{c}+\cdots+\bar{c}^{k-k_{j-1}})$, ε_3是一个任意小的正数, M_3是一个正数. 令$d_4=1-\rho M_3+\varepsilon_4$.

由式(34)和式(36)可得

$$\|\boldsymbol{e}(k)\|\leqslant d_3\boldsymbol{e}(k_{j-1}). \tag{38}$$

则上式意味着在DoS干扰攻击下输出信号不完全传输失败的情况下, 所提出的补偿算法可以保证系统输出误差有界且收敛.

注 6　DoS干扰攻击下MFAC算法的误差收敛率为

$$1-\frac{\rho b\bar{b}_1}{\lambda+\bar{b}_1^2},$$

而DoS干扰攻击下带有补偿的MFAC算法的误差收敛率为

$$1-\frac{\rho b\bar{b}_1}{\lambda+\bar{b}_1^2}d_3=1-\frac{\rho b\bar{b}_1}{\lambda+\bar{b}_1^2}(1+\bar{c}+\cdots+\bar{c}^{k-k_{j-1}}).$$

通过对比在发生DoS干扰攻击和随机丢包下不带补偿的MFAC算法的误差收敛率和带有补偿的MFAC算法的误差收敛率, 可得出带有补偿的MFAC算法的收敛速度更快, 更快的达到期望轨迹输出. 在仿真验证中也可得出.

5　仿真示例

1)　数值仿真.

考虑如下MIMO离散时间非线性系统:

$$\begin{cases}x_{11}(k+1)=\dfrac{x_{11}^2(k)}{1+x_{11}^2(k)}+0.4x_{12}(k),\\ x_{12}(k+1)=\\ \dfrac{x_{11}^2(k)}{1+x_{12}^2(k)+x_{21}^2(k)+x_2^2(k)}+l_1(k)u_1(k),\\ x_{21}(k+1)=\dfrac{x_{21}^2(k)}{1+x_{21}^2(k)}+0.4x_{22}(k),\\ x_{22}(k+1)=\\ \dfrac{x_{21}^2(k)}{1+x_{11}^2(k)+x_{12}^2(k)+x_{22}^2(k)}+l_2(k)u_2(k),\\ y_1(k)=x_{11}(k+1),\\ y_2(k)=x_{21}(k+1).\end{cases}$$

其中两个时变参数分别是

$$\begin{cases}l_1(k)=1+0.1\sin(2\pi k/1500),\\ l_2(k)=1+0.1\cos(2\pi k/1500).\end{cases}$$

该系统是一个时变耦合非线性系统. 期望轨迹如下:

$$\begin{cases}y_1^*=0.5+0.25\cos(0.25\pi k/100)+\\ \qquad 0.25\sin(0.5\pi k/100),\\ y_2^*=0.5+0.25\sin(0.25\pi k/100)+\\ \qquad 0.25\sin(0.5\pi k/100).\end{cases}$$

假设攻击者一个工作周期持续时间是T=100, 每个工作周期的休眠期持续时间$t_{\text{off}}=50$, 总的运行时间为1500, 因此运行周期为$n\in\{1,2,\cdots,15\}$. 假设攻击者处于休眠期系统的数据传输成功率为0.9, 处于攻击期系统的数据传输成功率下降为0.6. 系统的初始条件为

$$x_{1,1}(j)=x_{2,1}(j)=0.5,\ x_{1,2}(j)=x_{2,2}(j)=0,$$
$$j=1,2,\ \boldsymbol{u}(1)=\boldsymbol{u}(2)=[0\ \ 0]^{\mathrm{T}}.$$

控制器参数初始值为

$$\hat{\boldsymbol{\Phi}}(1)=\hat{\boldsymbol{\Phi}}(2)=\begin{bmatrix}0.5 & 0\\ 0 & 0.5\end{bmatrix};$$
$$\eta=\rho=1,\ \mu=1,\ \lambda=0.5.$$

仿真结果如图3所示.

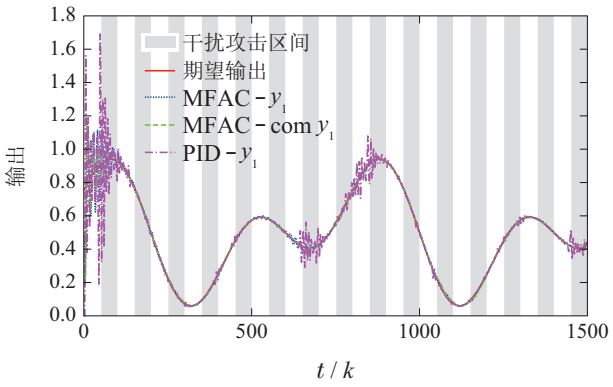

图 3　DoS干扰攻击下$y_1(k)$的跟踪性能

Fig. 3　Tracing performance of $y_1(k)$ under DoS attack

系统输出仿真结果如图3–4所示, 图中灰色阴影部分表示DoS干扰攻击区间. 由图3–4可以看出, 在仿真初期, 系统输出的超调量和波动范围较大, 表示系统受到DoS干扰攻击和随机丢包的影响, 发生波动. 随着时间的更新, 系统输出逐渐达到期望输出. 通过与PID控制对比, 可以看出本文设计的控制算法加快系统输出收敛速度.

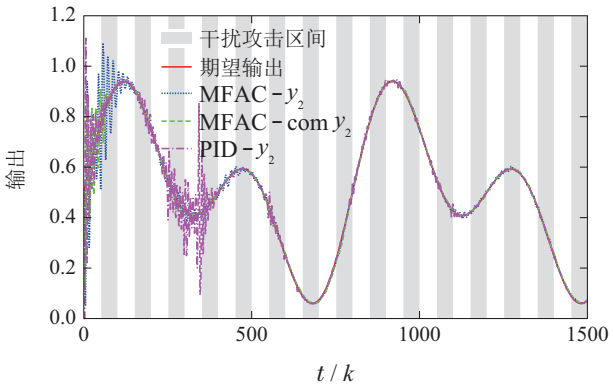

图 4　DoS干扰攻击下$y_2(k)$的跟踪性能

Fig. 4　Tracing performance of $y_2(k)$ under DoS attack

系统跟踪误差如图5所示, 跟踪误差在初始阶段波动较大, 但是随着时间的更新, 系统跟踪误差逐渐收敛. 图6中数字1–15代表攻击者完整的15个工作周期. 火柴棍代表数据传输失败时刻, 火柴棍的不同高度表

示攻击者处于不同的时期. 红色长棍在休眠区间, 蓝色短棍在攻击区间. 显然, 在休眠期火柴棍的分布更稀疏, 而在攻击期分布更为密集.

由数值仿真结果可以看出系统在遭受DoS干扰攻击和随机丢包情况下, 初始阶段系统输出跟踪性能较差, 但随着时刻的更新, 所提出的控制算法能够保证闭环系统有良好的跟踪性能, 通过补偿算法对系统控制输入的补偿, 最终系统可以更好的达到期望输出, 误差渐近收敛于0. 通过与PID仿真结果对比, 不仅验证了算法的有效性而且突出了本文算法的优越性.

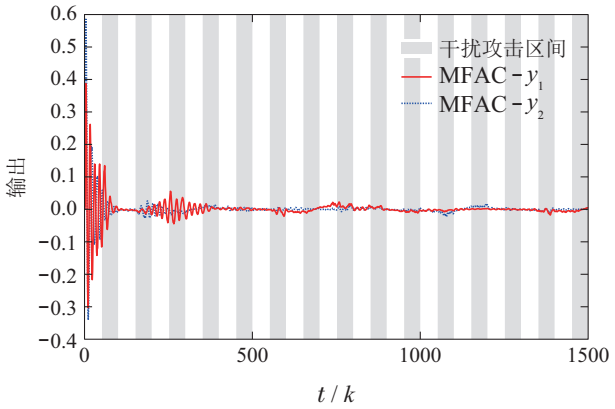

图 5 跟踪误差

Fig. 5 Tracking Error

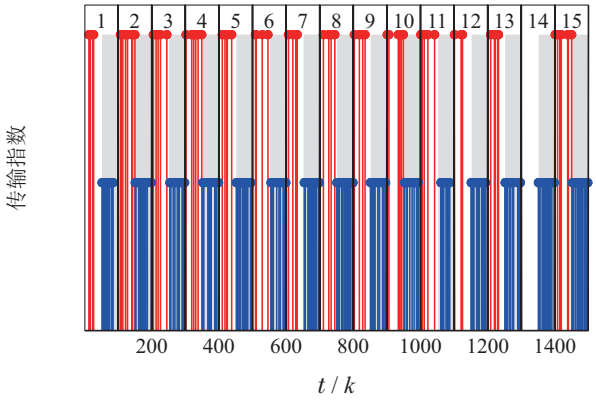

图 6 数据传输失败时刻

Fig. 6 Time of data transmission failure

2) 逆变器控制系统仿真.

逆变器控制系统如图7所示, 由直流电源、逆变桥、LC滤波电路构成, 其中, E是直流电源电压, V是逆变桥交流侧电压, $i_{\rm L}$是滤波电感电流, $i_{\rm R}$是负载电流, $V_{\rm C}$是滤波电容电压. 数据采集器通过电力线采集数据通过网络控制系统传输, 脉冲发生器根据控制输入信号产生适当宽度脉冲, 驱动逆变桥动作, 从而获得期望的交流输出电压.

逆变器系统可表述为

$$\begin{cases} C\dfrac{{\rm d}v_{\rm C}}{{\rm d}t} = i_{\rm L} - i_{\rm R}, \\ L\dfrac{{\rm d}i_L}{{\rm d}t} = V - v_{\rm C}. \end{cases}$$

将电容电压$v_{\rm c}$和电感电流$i_{\rm L}$作为输出变量$\boldsymbol{y} = [v_{\rm C}\ \ i_{\rm L}]$, 逆变器交流侧电压和负载电流作为输入变量$\boldsymbol{u} = [V\ \ i_{\rm R}]$. 仿真中逆变器直流侧电压$E = 400$ V, 滤波电感$L = 2.5$ mH, 滤波电容$C = 60$ μF, 参考电压$v_{\rm r} = 220\sqrt{2}\sin(100\pi k)$. 逆变控制系统期望输出如下

$$\begin{cases} y_1^*(k) = 220\sqrt{2}\sin(100\pi k), \\ y_2^*(k) = 52\sin(100\pi k). \end{cases}$$

假设攻击者一个工作周期持续时间为$T = 50$, 休眠持续时间$t_{\rm off} = 25$, 总的运行时间为600, 即运行周期$n \in \{1, 2, \cdots, 12\}$. 假设攻击者处于休眠期系统的数据传输成功率为0.9, 处于攻击期间系统的数据传输成功率下降为0.6. MFAC算法控制器参数设置如下η =0.5, ρ=0.5, μ=1, λ=0.01. PJM估计值的初值为

$$\hat{\boldsymbol{\Phi}}(1) = \hat{\boldsymbol{\Phi}}(2) = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.5 \end{bmatrix}.$$

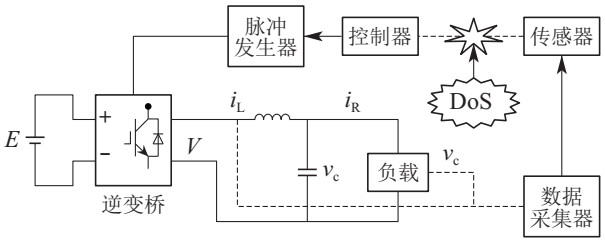

图 7 逆变器控制系统结构

Fig. 7 Inverter control system structures

图8–11表示逆变器控制系统仿真结果. 如图8所示, 本文设计的控制算法在发生DoS干扰攻击和随机丢包下可以保持电压稳定输出, 而通过补偿算法对控制输入进行补偿, 系统的输出电压可以更好的达到期望值. 图9是逆变器输出电流波形图, 在遭受DoS干扰攻击下电流幅值波动较大, 通过与PID对比可知补偿算法可以加快系统的收敛速度. 图10是误差跟踪图, 系统的跟踪误差曲线图随着时间更新逐渐平稳. 图11是DoS干扰攻击下控制系统数据传输失败时刻, 红色代表休眠期数据传输失败时刻, 蓝色代表攻击期数据传输失败时刻.

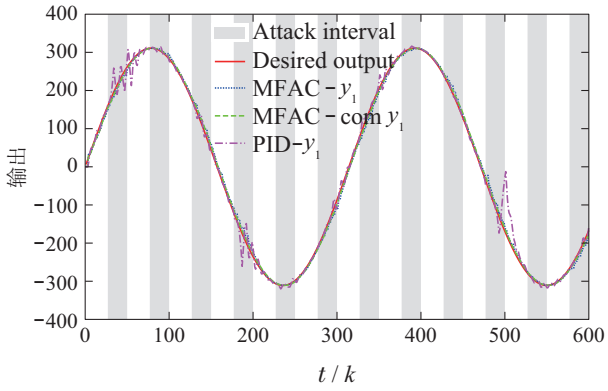

图 8 DoS干扰攻击下逆变器输出电压图形

Fig. 8 Inverter output voltage graph under DoS attack

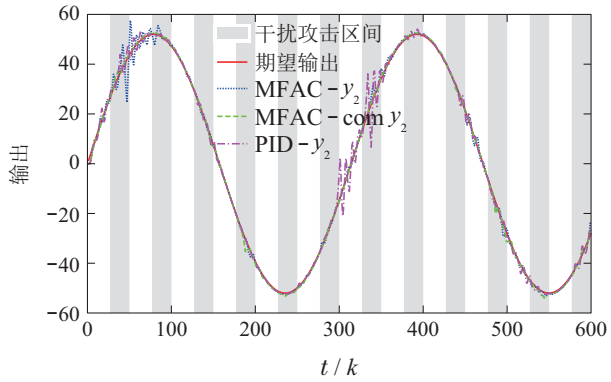

图 9　DoS干扰攻击下逆变器输出电流图形

Fig. 9　Inverter output current graph under DoS attack

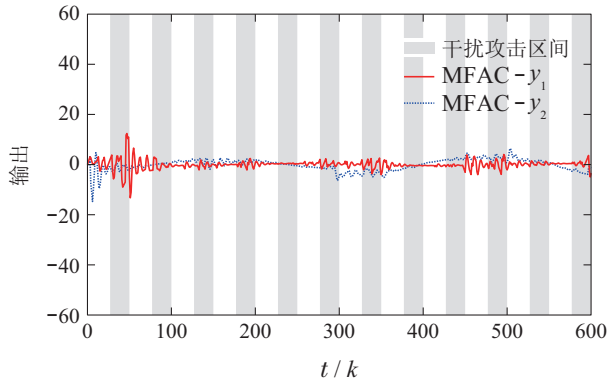

图 10　跟踪误差

Fig. 10　Tracking Error

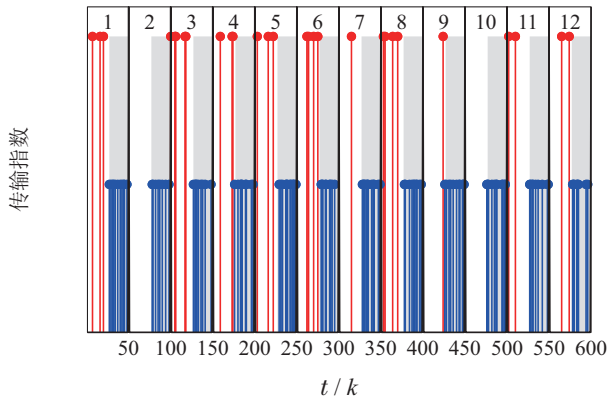

图 11　数据传输失败时刻

Fig. 11　Time of data transmission failure

仿真结果显示出周期性DoS攻击和数据包丢失会降低系统数据传输成功率, 降低系统的稳定性. 本文提出的MFAC算法可以有效抵消DoS干扰攻击给跟踪性能带来的负面影响, 仿真结果验证了算法的有效性, 而且通过与PID算法仿真结果的对比, 更好的展现出了算法的优越性.

6　结论与展望

本文针对MIMO非线性系统, 提出一种基于周期性DoS干扰攻击和随机丢包的无模型自适应控制算法. 首先通过引入伯努利分布对周期性DoS干扰攻击和随机丢包进行建模, 结合MIMO非线性系统设计控制算法, 其次通过数学推导分析了算法的收敛性, 最后仿真结果表明所提出的控制算法在DoS干扰攻击下仍然可以保证系统的稳定性, 并且补偿算法可以减轻DoS 攻击对控制系统的影响, 加快系统收敛速度, 此外该算法是数据驱动的不依赖系统的模型信息, 仅用系统I/O数据. 缺点是在DoS攻击下数据更新失败时系统仍然会传输历史数据, 从而造成网络资源的浪费. 如何在DoS干扰攻击环境下针对MIMO非线性系统设计事件触发机制, 减少系统通信资源的浪费, 这将是以后研究重点.

参考文献:

[1] JIN Shangtai, HOU Zhongsheng, CHI Ronghu, et al. Data driven model-free adaptive iterative learning control for a class of discrete time nonlinear systems. *Control Theory & Applications*, 2012, 29(8): 1001 – 1009.
(金尚泰, 侯忠生, 池荣虎, 等. 离散时间非线性系统的数据驱动无模型自适应迭代学习控制. 控制理论与应用, 2012, 29(8): 1001 – 1009.)

[2] CHI R, HOU Z. A model-free periodic adaptive control for freeway traffic density via ramp metering. *Acta Automatica Sinica*, 2010, 36(7): 1029 – 1033.

[3] LI Y, LIU Q, MENG W, et al. MISO model free adaptive control of single joint rehabilitation robot driven by pneumatic artificial muscles. *IEEE/ASME International Conference on Advanced Intelligent Mechatronics*. Boston, USA: IEEE, 2020: 1700 – 1705.

[4] XU Dezhi, DENG Jing, YAN Wenxu, et al. Data-driven path following constraint control for automatic overtaking system of intelligent vehicle. *Control Theory & Applications*, 2018, 35(2): 283 – 290.
(许德智, 邓竞, 颜文旭, 等. 智能车辆自动超车系统的数据驱动路径跟踪约束控制. 控制理论与应用, 2018, 35(2): 283 – 290.)

[5] ZHANG H, ZHOU J, SUN Q, et al. Data-driven control for interlinked AC/DC microgrids via model-free adaptive control and dual-droop control. *IEEE Transactions on Smart Grid*, 2017, 8(2): 557 – 571.

[6] CETINKAYA A, ISHII H, HAYAKAWA T. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 2017, 62(5): 2434 – 2449.

[7] BU X, HOU Z, HOU Z, et al. Robust iterative learning control design for linear systems with time-varying delays and packet dropouts. *Advances in Difference Equations*, 2017, 84: 1 – 17.

[8] MAHMOUD M, HAMDAN M. Fundamental issues in networked control systems. *IEEE Journal of Automatica Sinica*, 2018, 5(5): 902 – 922.

[9] BU X, HOU Z, JIN S. An iterative learning control design approach for networked control systems with data dropouts. *International Journal of Robust and Nonlinear Control*, 2016, 26(1): 91 – 109.

[10] SUN Q, ZHANG K, SHI Y. Resilient model predictive control of cyber-physical systems under DoS attacks. *IEEE Transactions on Industrial Informatics*, 2020, 16(7): 4920 – 4927.

[11] YU W, WANG R, BU X, et al. Model free adaptive control for a class of nonlinear systems with fading measurements. *Journal of the Franklin Institute*, 2020, 357(12): 7743 – 7760.

[12] DING D, WANG Z, WEI G, et al. Event-based security control for discrete-time stochastic systems. *IET Control Theory & Applications*, 2016, 10(15): 1808 – 1815.

[13] YE D, ZHANG T, GUO G. Stochastic coding detection scheme in cyber-physical systems against replay attack. *Information Sciences*, 2019, 481: 432 – 444.

[14] HU S, DONG Y, XIE X. Resilient event-triggered controller synthesis of networked control systems under periodic DoS jamming attacks. *IEEE Transactions on Cybernetics*, 2019, 49(12): 4271 – 4281.

[15] WANG Mufeng. Research on stabilization and control of cyber-physical systems under DoS interference attack. *Control and Decision*, 2019, 34(8): 1681 – 1687.
(汪慕峰. DoS干扰攻击下的信息物理系统镇定与控制研究. 控制与决策, 2019, 34(8): 1681 – 1687.)

[16] FOROUSH H, MARTINEZ S. On triggering control of single-input linear systems under pulse-width modulated DoS signals. *SIAM Journal on Control & Optimization*, 2016, 54(6): 3084 – 3105.

[17] ZHANG X, HAN Q L, GE X, et al. Resilient control design based on a sampled-data model for a class of networked control systems under denial-of-service attacks. *IEEE Transactions on Cybernetics*, 2020, 50(8): 3616 – 3626.

[18] LU A, YANG G. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial-of-service. *IEEE Transactions on Automatic Control*, 2018, 16(6): 1813 – 1820.

[19] FOROUSH H, MARTINEZ S. On muli-input controllable linear systems under periodic DoS jamming attacks. *Proceedings of the Conference on Control and its Application*, California, USA: SIAM, 2013: 222 – 229.

[20] GU Z, AHN C, YUE D, et al. Event-triggered H_∞ filtering for T-S fuzzy-model-based nonlinear networked systems with multisensors against DoS attacks. *IEEE Transactions on Cybernetics*, 2020, P-P(99): 1 – 11.

[21] HOU Z, JIN S. Data-driven model-free adaptive control for a class of MIMO nonlinear discrete-time systems. *IEEE Transactions on Neural Networks*, 2011, 22(12): 2173 – 2188.

[22] GERSCHGORIN S. *Uber die Abgrenzung der Eigenwerte Einer Matrix*. Izv, Akad. Nauk. USSR Otd. Fiz. Mat. Nauk 7, 1931: 749 – 754.

[23] HUANG L. *Linear Algebra in Systems and Control Theory.* Beijing: Science Press, 1984.

作者简介:

赵栩杨 硕士研究生, 目前研究方向为信息处理与网络控制、无模型自适应控制等, E-mail: 1789610350@qq.com;

卜旭辉 教授, 目前研究方向为数据驱动控制、迭代学习控制、交通控制、网络系统控制等, E-mail: buxuhui@gmail.com;

余 威 硕士研究生, 目前研究方向为无模型自适应控制、迭代学习控制、网络系统控制等, E-mail: yuwei5150@163.com;

游东亚 硕士研究生, 目前研究方向为工业过程控制、数据驱动控制、迭代学习控制等, E-mail: youdy123@foxmail.com.