列车控制系统的抗拒绝服务攻击弹性控制策略

高　兵†, 步　兵

(北京交通大学 轨道交通控制与安全国家重点实验室, 北京 100044)

摘要: 当遭受拒绝服务(DoS)攻击时, 分布式列车控制系统的弹性控制问题受到广泛关注. 本文提出了一种基于分布式领导车状态观测器和障碍李雅普诺夫函数的弹性控制策略, 不仅可以避免列车碰撞, 同时实现了编队控制的目标. 首先, 给出了一种分布式的领导车状态观测器设计方法, 用于实时估计领导车的状态. 理论分析表明, 在DoS攻击满足一定约束的条件下, 该状态观测器的估计误差具有指数稳定特性. 在此基础上, 通过将列车碰撞避免问题转化为状态受限问题, 提出一种基于障碍李雅普诺夫函数的状态受限控制律, 解决了DoS攻击下确保碰撞避免的车队控制问题. 最后, 数值仿真证实了本文方法的有效性.

关键词: 拒绝服务; 弹性控制; 状态估计; 障碍李雅普诺夫函数; 列车运行控制; 碰撞避免

引用格式: 高兵, 步兵. 列车控制系统的抗拒绝服务攻击弹性控制策略. 控制理论与应用, 2024, 41(2): 311 – 320

DOI: 10.7641/CTA.2023.20255

Resilient control strategy for the train control system against denial of service attacks

GAO Bing†, BU Bing

(State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing 100044, China)

Abstract: When suffering from the denial of service (DoS) attacks, the resilient control problem of distributed train control systems has attracted widespread attention. In this paper, a resilient control strategy based on the distributed state observer of the leader train and the barrier Lyapunov function is proposed, which can not only avoid train collisions, but also achieve the platoon control objective. Firstly, under DoS attacks, a distributed state observer of the leader train is proposed to estimate the states of the leader train in real time. Theoretical analysis shows that the estimated error of the state observer is exponentially stable on the condition that the DoS attack satisfies certain constraints. On this basis, by transforming the train collision avoidance problem into a state-constrained problem, a state-constrained control law based on the barrier Lyapunov function is proposed, which solves the resilient platoon control problem, to ensure collision avoidance under DoS attacks. Finally, numerical simulation confirms the effectiveness of the proposed method.

Key words: denial of service; resilient control; state estimation; barrier Lyapunov function; train operation control; collision avoidance

Citation: GAO Bing, BU Bing. Resilient control strategy for the train control system against denial of service attacks. *Control Theory & Applications*, 2024, 41(2): 311 – 320

1　引言

近年来, 随着自动列车技术和车车通信技术的进步, 智能交通作为一个新的研究热点, 得到了科研和产业界的广泛关注和投入. 智能交通提高了司机驾驶的舒适度, 增大了交通吞吐量, 节约了燃料, 同时减少了交通管理所需要的人力和物力. 然而, 在实际推广前, 必须解决智能交通系统遭受恶意攻击时的信息安全问题. 由于车辆间使用无线通信技术传输列车自动控制所需要的状态信息等重要信息, 使得关键的列车控制信息暴露在无线通信的攻击面下, 增加了信息安全风险[1–2]. 为抵抗恶意的信息安全风险, 智能交通系统主要使用3种方法: 第1种是研究入侵检测方法来及时检测攻击; 第2种是研究相应的认证机制等来加强信息传输的安全性; 第3种是研究如何从控制的角度

收稿日期: 2022−04−10; 录用日期: 2023−03−21.
†通信作者. E-mail: 17111041@bjtu.edu.cn.
本文责任编委: 俞立.
北京市自然科学基金–丰台轨道交通前沿研究联合基金项目(L211002), 先进轨道交通自主运行全国重点实验室自主课题项目(RAO2023ZZ004), 城市轨道交通北京实验室资助.
Supported by the Beijing Natural Science Foundation-Fengtai Rail Transit Frontier Research Joint Fund (L211002), the State Key Laboratory of Advanced Rail Autonomous Operation (RAO2023ZZ004) and the Beijing Laboratory for Urban Mass Transit.

去缓解攻击造成的影响, 保证列车以可容忍的性能运行并提高列车运行效率, 也就是采用弹性控制的方法去抵抗恶意的信息安全风险.

作为第3种研究方法, 即恶意攻击下的弹性控制问题, 近年来成为一个研究热点, 可有效解决攻击下车队的安全控制问题. 所谓弹性控制, 是指针对结构、参数等变化引起的波动, 包括恶意攻击和极端干扰, 系统在一定范围内以可接受的状态维持系统运行的控制能力, 以及一旦波动消失时系统性能可快速恢复的控制能力[3].

针对恶意攻击下的弹性控制问题, 目前已经有了一些成果. 针对车车通信链路遭受恶意欺骗攻击、数据篡改攻击和拒绝服务攻击等情况, 文献[4]提出了一个基于同步的自适应协同控制策略以确保车队中的车以期望的速度和加速度安全运行. 然而, 当车队同步未实现时, 自适应协同控制的增益是单调增长的. 因此, 该自适应控制算法本质上是高增益的, 对测量噪声和干扰非常敏感. 文献[5]考虑了有通信延迟和跟驰作用时的轨迹跟踪弹性控制问题, 提出了一种分布式非线性轨迹跟踪控制方法. 然而, 由于要求领导车为匀速行驶且系统通信时延已知, 这个假设在实际中很难满足. 针对传器感和执行器同时被攻击的情况, 在传感器和执行器的攻击模型具有线性参数不确定形式的假设下, 文献[6]提出了一个带有校正信号的自适应反馈控制器, 确保闭环系统是一致最终有界的. 文献[7]研究了拒绝服务 (denial of service, DoS) 攻击下车队的弹性协同自适应巡航控制(cooperative adaptive cruise control, CACC)问题, 这里DoS攻击被建模成随机延迟, 假设DoS攻击只攻击来自前车的速度和加速度, 前车的位置假设是可靠传输的. 该算法使用时延估计器估计DoS攻击引起的随机时延. 基于估计的时延, 使用观测器得到具有一定可信度的前车状态. 时延估计器基于状态估计残差去更新时延估计并反馈给观测器. 需要注意的是, 由于假设前车的位置始终是可靠传输的, 这个条件是比较苛刻的. 针对同样的问题, 文献[8]提出了一种基于线性矩阵不等式的控制器调整算法以寻找控制器的最佳增益. 在给定控制器增益的情况下, 该调整算法给出了最大允许连续丢包数的下限, 从而识别了系统能克服的最严重的DoS攻击情况. 然而, 这里仅仅假设来自前车的控制指令传输被攻击, 前车的位置和速度仍然可以正常传输. 文献[9]研究了网络攻击下车队系统的一致性问题, 攻击的影响是导致车辆状态存在一定的偏差. 该文献通过引入一个虚拟层, 提出了一个由原始车队层和虚拟层组成的交互式网络框架以抵抗攻击的影响. 在攻击引起的偏差为有限L_2增益的情况下, 给出了一个充分必要条件, 使得状态误差收敛在一个有界的范围. 针对DoS攻击下的车队控制问题, 文献[10]提出了一个基于一致性的分布式事件触发控制律, 并给出了一个可同时得到控制器参数和事件触发条件的协同设计算法. 针对执行机构存在饱和等物理约束的事实, 文献[11]给出了一种设计执行器新饱和边界的方法, 使得新的外椭球边界尽可能大, 同时保证危险状态不可到达, 以最大限度地减少系统性能的损失. 针对采用事件触发通信机制和CACC控制器的车队系统, 文献[12]提出了一个滑模观测器实现对网络攻击的检测和估计, 并证明了该观测器的稳定性和检测阈值的鲁棒性. 文献[13]研究无线通信的不确定性和堵塞攻击对车队稳定性和安全性的影响, 基于CACC的网络–物理状态耦合模型, 提出了一种新的时域方法来分析系统的车队稳定性, 并分析了堵塞攻击的位置对车队稳定性的影响. 结果表明, 堵塞攻击越靠近领导车, 恶意干扰则有更高的概率使车队失稳. 针对存在DoS攻击和多重干扰的车队控制问题, 文献[14]提出了一个弹性控制律以确保车队稳定性, 该弹性控制律跟攻击的持续时间和发生次数有关.

需要说明的是, 上述攻击下的弹性车队控制方法, 绝大多数只关注闭环系统的渐近稳定性等问题, 无法从理论上确保列车之间满足一定的安全距离, 也就是无法确保相邻列车间的碰撞避免问题. 或者只是单纯地研究碰撞避免问题, 而不关注弹性性能. 基于这个动机, 本文提出了一种抗DoS攻击的弹性编队控制方法, 把列车碰撞避免问题转化成前后车的距离大于最小安全距离的状态约束问题, 通过引入障碍李雅普诺夫函数将基于估计的列车编队的弹性控制问题和碰撞避免问题巧妙地结合起来, 从控制的角度解决了列车自主控制系统的主要关切. 具体地, 本文通过在各个跟随车上部署状态观测器实时估计领导车的状态. 利用估计的领导车状态, 设计了基于障碍李雅普诺夫函数的状态受限控制律, 解决了碰撞避免下的车队弹性控制问题.

2 问题描述

本节首先给出了列车动力学模型和车车通信模型. 进一步, 给出了DoS攻击模型. 最后, 给出了本文的控制目标.

2.1 列车动力学建模

基于车车通信的列车控制系统可采用车队控制的方式运行. 假设列车个数为$n+1$. 对每个列车而言, 它的动力学方程如下:

$$\dot{s}_i = v_i, \tag{1a}$$

$$\dot{v}_i = a_i, \tag{1b}$$

$$\dot{a}_i = -\frac{1}{\tau}a_i + \frac{1}{\tau}a_i^{\mathrm{c}}, \tag{1c}$$

其中: s_i, v_i和a_i分别表示列车i的位置、速度和加速度, $i = 0, 1, \cdots, n$; 式(1c)为执行机构动力学, 此处假

设为1阶惯性环节, τ为时间常数且$\tau > 0$, a_i^{c}为控制输入.

在所有$n+1$个列车中, 第0个车称为领导车, 其他车称为跟随车. 对领导车, 定义状态$x_0 = [s_0\ \ v_0\ \ a_0]^{\mathrm{T}}$, 控制输入$u_0 = a_0^{\mathrm{c}}$以及输出$y_0 = x_0$, 设计如下控制律:

$$u_0 = k_{0,1}\,(y_{\mathrm{r}} - x_{0,1}) + k_{0,2}\,(\dot{y}_{\mathrm{r}} - x_{0,2}) + \ddot{y}_{\mathrm{r}}, \tag{2}$$

其中: $k_{0,j}$为控制参数, 满足$k_{0,j} > 0$, $j = 1, 2$; $x_{0,i}$是x_0的第i个元素, 也即$x_0 = [x_{0,1}\ \ x_{0,2}\ \ x_{0,3}]^{\mathrm{T}}$; y_{r}为领导车的位置参考曲线, $\dot{y}_{\mathrm{r}}$和$\ddot{y}_{\mathrm{r}}$分别是它的一阶导数和二阶导数. 关于位置参考曲线y_{r}, 作如下假设.

假设 1　位置参考曲线的前三阶导数$\dot{y}_{\mathrm{r}}$, $\ddot{y}_{\mathrm{r}}$和$y_{\mathrm{r}}^{(3)}$是有界的.

定义

$$\delta = x_0 - [y_{\mathrm{r}}\ \ \dot{y}_{\mathrm{r}}\ \ \ddot{y}_{\mathrm{r}}]^{\mathrm{T}}, \tag{3}$$

表示领导车的状态与它的参考曲线之间的跟踪误差. 对δ求导, 并将领导车的动力学方程(1a)–(1c)和控制律(2)代入, 得到下述闭环跟踪误差方程:

$$\dot{\delta} = S\delta + B(-\tau y_{\mathrm{r}}^{(3)}), \tag{4}$$

其中: S和B分别定义如下:

$$S = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -\dfrac{k_{0,1}}{\tau} & -\dfrac{k_{0,2}}{\tau} & -\dfrac{1}{\tau} \end{bmatrix},\ B = \begin{bmatrix} 0 \\ 0 \\ \dfrac{1}{\tau} \end{bmatrix}. \tag{5}$$

关于闭环跟踪误差方程(4), 有下面的引理.

引理 1　在假设1成立的前提下, 考虑闭环跟踪误差方程(4). 如果S是赫尔维兹矩阵, 则δ是有界的. 进一步, 如果领导车的位置参考曲线y_{r}的三阶导数$y_{\mathrm{r}}^{(3)}$指数收敛到零, 则δ也指数收敛到零.

2.2　车车通信拓扑建模

对于采用车车通信的基于车车通信的列车自主运行系统(train autonomous circumambulate system, TACS)而言, 其通信拓扑可以采用图论相关知识进行描述. 具体地, 定义有向图$\mathcal{G} = \{V, E\}$, 其中$V = \{0, 1, \cdots, n\}$为列车节点集, $E = V \times V$为边集, 表征各个列车之间的通信连接情况, 若$(i, j) \in E$, 说明列车i可以向列车j传输消息.

针对有向图$\mathcal{G}$, 定义邻接矩阵$\mathcal{A} = [a_{ij}] \in \mathbb{R}^{n\times n}$表征任意两个跟随车之间的通信关系, 其中$a_{ij}(i, j \in \{1, 2, \cdots, n\})$定义如下:

$$a_{ij} = \begin{cases} 1,\ (j, i) \in E, \\ 0,\ \text{其他}. \end{cases} \tag{6}$$

进一步, 定义跟随车的入度矩阵为

$$\mathcal{D} = \mathrm{diag}\{d_1, d_2, \cdots, d_n\}, \tag{7}$$

其中: 符号"diag"表示对角阵, $d_i = \sum\limits_{j=1}^{n} a_{ij}$, $i \in \{1,2, \cdots, n\}$.

根据邻接矩阵$\mathcal{A}$和入度矩阵$\mathcal{D}$, 定义如下的拉普拉斯矩阵$\mathcal{L}$:

$$\mathcal{L} = -\mathcal{A} + \mathcal{D}, \tag{8}$$

最后, 定义$\mathcal{H}$表示各跟随车与领导车的连接矩阵, 即

$$\mathcal{H} = \mathrm{diag}\{h_1, h_2, \cdots, h_n\}, \tag{9}$$

其中$h_i = 1$意味着$(0, i) \in E$, 也即跟随车i可以收到领导车的信息, 否则$h_i = 0$.

对于一个列车编队系统而言, 整个车队的通信拓扑记为$\mathcal{G}_j$, $j \in \{1, 2, \cdots, n\}$. 由于DoS攻击会导致列车之间的通信链路中断, 因此整个车队的通信拓扑是时变的. 总体来说, 通信拓扑可分为两类[14]: 一类称为生成树保持型通信拓扑, 即通信拓扑中至少存在一颗生成树, 此时列车之间是连通的; 另一类称为生成树瘫痪型通信拓扑, 此时通信拓扑不存在生成树. 在所有的通信拓扑中, 将生成树保持型通信拓扑对应的序号组成的集合记为C_{m}, 将生成树瘫痪型通信拓扑对应的序号记为C_{p}. 为了简化描述, 后续直接用C_{m}和C_{p}表示这两类拓扑.

对生成树保持型通信拓扑, 作如下假设.

假设 2　对任何生成树保持型通信拓扑C_{m}, 领导车都是生成树的根节点.

2.3　DoS攻击建模

DoS攻击通过破坏通信对象之间数据的完整性或利用系统中设备的漏洞来阻止正常的信息交换[2]. 因此, 对于列控系统而言, DoS攻击将中断通信连接, 导致出现生成树瘫痪型通信拓扑$\mathcal{G}_{\sigma(t)}$, $\sigma(t) \in C_{\mathrm{p}}$.

针对DoS攻击, 用$\mathcal{T}_{\mathrm{p}}(t_1, t_2)$和$\mathcal{N}_{\mathrm{p}}(t_1, t_2)$分别表示在时间区间$[t_1, t_2)$内生成树瘫痪型通信拓扑的持续时间和发生次数, 这里$t_2 > t_1 > 0$. 引入下面两个定义[14].

定义 1　$\dfrac{\mathcal{T}_{\mathrm{p}}(t_1, t_2)}{t_2 - t_1}$表示在时间区间$[t_1, t_2)$上, 生成树瘫痪型通信拓扑的时间占比, 其中$t_2 > t_1 > 0$.

定义 2　$\mathcal{F}_{\mathrm{p}}(t_1, t_2) = \dfrac{\mathcal{N}_{\mathrm{p}}(t_1, t_2)}{t_2 - t_1}$表示在时间区间$[t_1, t_2)$上, 生成树瘫痪型通信拓扑的发生频率, 其中$t_2 > t_1 > 0$.

2.4　控制目标

本文的控制目标是针对基于车车通信的列车控制系统, 考虑DoS攻击存在的情况, 要求在避免列车碰撞的前提下, 稳态时所有相邻列车保持一个期望的固定间隔, 即对所有的列车i $(i = 1, 2, \cdots, n)$有

$$s_{i-1}(t) - s_i(t) > \Delta S,\ \forall t > 0, \tag{10a}$$

同时,

$$\begin{cases}\lim\limits_{t\to\infty}\|s_{i-1}(t)-s_i(t)-d\|=0,\\ \lim\limits_{t\to\infty}\|v_i(t)-v_0(t)\|=0,\\ \lim\limits_{t\to\infty}\|a_i(t)-a_0(t)\|=0,\end{cases}\tag{10b}$$

其中: ΔS表示相邻列车间的最小安全距离, d为期望的列车间隔, v_0和a_0分别表示领导车的速度和加速度.

3 控制器设计

本节给出DoS攻击下的弹性控制策略. 首先, 提出一种分布式领导车状态观测器, 用于各个跟随车对领导车的状态进行估计. 基于估计的领导车状态, 进一步给出了一种基于障碍李雅普诺夫函数的控制器设计方法, 从而在避免列车碰撞的情况下实现了车队的弹性控制.

3.1 分布式领导车状态观测器设计

将领导车的控制律(2)代入领导车的动力学方程(1a)–(1c)中, 得到领导车的闭环方程为

$$\dot{x}_0=Sx_0+By_{\mathrm{r}}^{\Delta},\tag{11}$$

其中: S和B定义见式(5); y_{r}^{Δ}为参考曲线y_{r}的相关项, 定义如下:

$$y_{\mathrm{r}}^{\Delta}=k_{0,1}y_{\mathrm{r}}+k_{0,2}\dot{y}_{\mathrm{r}}+\ddot{y}_{\mathrm{r}}.\tag{12}$$

基于闭环方程(11), 在跟随车i上, 设计如下观测器以估计领导车状态:

$$\dot{\zeta}_i=S\zeta_i+B\zeta_i^{\Delta}+\varphi(\sum_{j=1}^{n}a_{ij}(\zeta_j-\zeta_i)+h_i(x_0-\zeta_i)),\tag{13}$$

其中: $\zeta_i=[\zeta_{i,1}\ \ \zeta_{i,2}\ \ \zeta_{i,3}]^{\mathrm{T}}\in\mathbb{R}^3$是列车$i$估计的领导车状态; φ为控制参数, 满足$\varphi>0$; a_{ij}和h_i分别在式(6)和式(9)中定义. 由于$\zeta_{i,1}$, $\zeta_{i,2}$和$\zeta_{i,3}$分别是领导车的位置、速度和加速度的估计, 参考式(12)中定义的y_{r}^{Δ}的形式, ζ_i^{Δ}定义如下:

$$\zeta_i^{\Delta}=k_{0,1}\zeta_{i,1}+k_{0,2}\zeta_{i,2}+\zeta_{i,3}.\tag{14}$$

下面分析领导车状态观测器式(13)的性能, 假设引理1满足. 定义整个车队的状态估计误差χ如下:

$$\chi=[\chi_1^{\mathrm{T}}\ \ \chi_2^{\mathrm{T}}\ \ \cdots\ \ \chi_n^{\mathrm{T}}]^{\mathrm{T}},\tag{15}$$

其中χ_i表示列车i对领导车的状态估计误差, 定义如下:

$$\chi_i=\zeta_i-x_0,\tag{16}$$

利用式(11)(13), 可得下面的估计误差方程:

$$\dot{\chi}=M\chi+\bar{B}\epsilon,\tag{17}$$

其中M, $\bar{B}$和ϵ分别定义如下:

$$\begin{cases}M=I_n\otimes\bar{A}-\varphi\left(\mathcal{W}\otimes I_3\right),\\ \bar{B}=[B^{\mathrm{T}}\ \ \cdots\ \ B^{\mathrm{T}}]^{\mathrm{T}}\in\mathbb{R}^{3\times n},\\ \epsilon=[k_{0,1}\ \ k_{0,2}\ \ 1]\delta,\end{cases}\tag{18}$$

其中: I_j表示j阶单位矩阵; 符号"$\otimes$"表示Kronecker积; $\bar{A}$定义如下:

$$\bar{A}=\begin{bmatrix}0&1&0\\0&0&1\\0&0&0\end{bmatrix};$$

$\mathcal{W}=\mathcal{L}+\mathcal{H}$, 其中: $\mathcal{L}$为通信拓扑的拉普拉斯矩阵, $\mathcal{H}$为各跟随车与领导车的连接矩阵, 分别在式(8)和式(9)中定义; B和δ的定义分别见式(5)和式(3). 根据引理1, 可知当$y_{\mathrm{r}}^{(3)}$指数收敛到零时, δ也指数收敛到零. 因此, 对于式(18)中的ϵ, 存在正常数ψ以及ϱ, 使得

$$|\epsilon(t)|\leqslant\psi\mathrm{e}^{-\varrho t}.\tag{19}$$

对任意的通信拓扑$r\in C_{\mathrm{m}}$, 即正常通信情况, 在假设2成立的前提下, 可知式(18)中的M是赫尔维兹矩阵[15]. 根据李雅普诺夫稳定性理论[16], 可知存在一个正定矩阵$P_r>0$和一个正常数$\beta_r>0$, 使得下式满足:

$$M^{\mathrm{T}}P_r+P_rM+\beta_rP_r<0,\ r\in C_{\mathrm{m}},\tag{20}$$

同时, 对任意的通信拓扑$r\in C_{\mathrm{p}}$, 即DoS攻击情况下, 可知M的特征值或者为零或者实部为负[15]. 根据Lyapunov稳定性理论[16], 存在正定矩阵$P_r>0$和正常数$\alpha_r>0$满足

$$M^{\mathrm{T}}P_r+P_rM-\alpha_rP_r<0,\ r\in C_{\mathrm{p}},\tag{21}$$

基于式(20)–(21), 定义

$$\rho=\frac{\lambda_{\max}^{P_r}}{\lambda_{\min}^{P_r}},\tag{22}$$

其中$\lambda_{\max}^{P_r}$和$\lambda_{\min}^{P_r}$分别定义如下:

$$\lambda_{\max}^{P_r}=\max\{\lambda(P_r),\ r\in C_{\mathrm{m}}\cup C_{\mathrm{p}}\},$$
$$\lambda_{\min}^{P_r}=\min\{\lambda(P_r),\ r\in C_{\mathrm{m}}\cup C_{\mathrm{p}}\},$$

式中$\lambda\left(P_r\right)$表示矩阵P_r的特征值.

针对车队系统的闭环估计误差方程(17), 选取如下李雅普诺夫函数:

$$V=\chi^{\mathrm{T}}P_r\chi,\tag{23}$$

其中P_r满足式(20)或者式(21). 若$r\in C_{\mathrm{m}}$, 也即此时为正常通信情况, 可知

$$\dot{V}\leqslant-L_1V+L_2,\tag{24}$$

其中L_1和L_2分别定义如下:

$$\begin{aligned}L_1&=\max_{r\in C_{\mathrm{m}}}\frac{\beta\lambda_{\min}(P_r)-\kappa}{\lambda_{\max}(P_r)},\\ L_2&=\frac{1}{\kappa}(\max_{r\in C_{\mathrm{m}}}\{\|P_r\|\}\|\bar{B}\|)^2\epsilon^2,\end{aligned}\tag{25}$$

式中: $\beta=\min\{\beta_r,\ r\in C_{\mathrm{m}}\}$, κ为一正常数, 满足$\kappa<\beta\lambda_{\min}(P_r)$. 若$r\in C_{\mathrm{p}}$, 也即此时遭受DoS攻击, 可知

$$\dot{V}\leqslant L_3V+L_4,\tag{26}$$

其中:

$$\begin{cases} L_3 = \max\limits_{r\in C_{\rm p}} \dfrac{\alpha\lambda_{\max}(P_r)+\kappa}{\lambda_{\min}(P_r)}, \\ L_4 = \dfrac{1}{\kappa}(\max\limits_{r\in C_{\rm p}}\{\|P_r\|\}\|\bar{B}\|)^2\epsilon^2, \end{cases} \tag{27}$$

式中$\alpha = \max\{\alpha_r,\ r\in C_{\rm p}\}$.

定义序列$\{\xi_k\}$ $(k=0,1,\cdots)$表示正常通信拓扑$C_{\rm m}$与DoS攻击下异常通信拓扑$C_{\rm p}$的切换时刻, 其中$\xi_0 = t_0$. 假设初始时刻系统未遭受DoS攻击, 则在时间区间(ξ_{2k},ξ_{2k+1})上, 系统可以正常通信, 此时通信拓扑为生成树保持型通信拓扑$C_{\rm m}$, 而在时间区间(ξ_{2k+1},ξ_{2k+2})上, 系统遭受DoS攻击, 此时通信拓扑为生成树瘫痪型通信拓扑$C_{\rm p}$, $k=0,1,\cdots$.

关于车队系统的闭环估计误差方程(17), 有下面的定理.

定理 1　假定引理1的条件满足, 即假设1成立, S是赫尔维兹矩阵, 以及领导车的位置参考曲线$y_{\rm r}$的3阶导数$y_{\rm r}^{(3)}$指数收敛到零. 进一步, 在假设2成立的前提下, 设计领导车控制律式(2)中的控制参数$k_{0,1}$和$k_{0,2}$使得式(19)中ϵ的外包络参数ϱ满足$\varrho > \dfrac{L_3}{2}$. 在此基础上, 任意选取$\varsigma\in(0,2\varrho-L_3)$, $\mu^*\in(0,L_1)$, $\mu\in(0,\mu^*)$, 如果DoS攻击的持续时间和频率满足下面各式:

$$\frac{\mathcal{T}_{\rm p}(\xi_{2l},\xi_{2p})}{\xi_{2p}-\xi_{2l}} < \frac{L_1-\mu^*}{L_1+L_3},\ 0\leqslant l<p, \tag{28}$$

$$\frac{\mathcal{T}_{\rm p}(\xi_{2l+1},\xi_{2p+1})}{\xi_{2p+1}-\xi_{2l+1}} < \frac{L_1-\mu^*}{L_1+L_3},\ \forall 0\leqslant l<p, \tag{29}$$

$$\mathcal{F}_{\rm p}(\xi_0,\xi_{2k}) < \frac{\min\{2\varrho-L_3-\varsigma,\mu^*-\mu\}}{2\ln\rho},\ \forall k>0, \tag{30}$$

同时, 在领导车状态观测器式(13)中, 任意选择$\varphi>0$, 则由式(17)描述的领导车状态观测器的跟踪误差指数收敛到零, 即存在正常数$\varUpsilon_1$和$\varUpsilon_2$, 使得

$$\|\ \chi(t)\ \|\leqslant \varUpsilon_1{\rm e}^{-\varUpsilon_2 t}\ \|\ \chi(0)\ \|, \tag{31}$$

式中: L_1, L_3和ρ分别在式(25)、式(27)和式(22)中定义; $\mathcal{T}_{\rm p}$和$\mathcal{F}_{\rm p}$的含义分别见第2.3节中的定义1和定义2.

证　选取李雅普诺夫函数如式(23)所示. 根据不等式(19), 可知表征领导车状态和它参考轨迹跟踪误差有关的ϵ满足$\epsilon\to 0$. 进一步, 可知在式(25)和式(27)中, 分别有$L_2\to 0$和$L_4\to 0$. 进一步结合式(24)和式(26), 可知当通信拓扑为生成树保持型通信拓扑$C_{\rm m}$时, 李雅普诺夫函数有收敛趋势, 当通信拓扑为生成树瘫痪型通信拓扑$C_{\rm p}$时, 李雅普诺夫函数有发散趋势. 结合时间序列$\{\xi_k\}$的定义, 可知最恶劣情况发生在ξ_{2l} $(l>0)$时刻. 因此, 只需要对$\xi_{2l}(l>0)$时刻进行分析即可.

在时间区间(ξ_0,ξ_1)上, 通信拓扑为$C_{\rm m}$, 此时有式(24)成立. 利用比较原理[17], 可知

$$V(\xi_1^-)\leqslant {\rm e}^{-L_1(\xi_1-\xi_0)}V(\xi_0) - \frac{L_2}{L_1}{\rm e}^{-L_1(\xi_1-\xi_0)} + \frac{L_2}{L_1},$$

在时间区间(ξ_1,ξ_2)上, 通信拓扑为$C_{\rm p}$, 此时有式(26)成立. 利用比较原理, 可知

$$V(\xi_2^-)\leqslant {\rm e}^{L_3(\xi_2-\xi_1)}V(\xi_1^+) + \frac{L_4}{L_3}{\rm e}^{L_3(\xi_2-\xi_1)} - \frac{L_4}{L_3},$$

由于在ξ_1处, 通信拓扑类型发生了切换, 式(23)所给的李雅普诺夫函数中P_r也发生了跳变. 考虑到闭环估计误差方程(17)中的状态χ是连续的, 因此有

$$V(\xi_1^+)\leqslant \rho V(\xi_1^-),$$

式中ρ的定义见式(22).

基于上述事实, 利用时间占比条件(28)–(29), 以及$\rho>1$, 不断迭代, 可得

$$\begin{aligned} V(\xi_{2k}^-) < {} & \rho^{2k-1}{\rm e}^{\varDelta(\xi_0,\xi_{2k})}V(\xi_0) - \\ & \frac{L_2}{L_1}\rho^{2k-1}{\rm e}^{\varDelta(\xi_0,\xi_{2k})} + \\ & \rho\frac{L_2}{L_1}{\rm e}^{\varDelta(\xi_{2k-1},\xi_{2k})}\frac{\rho^{2k}}{\rho^2-1} + \\ & \frac{L_4}{L_3}{\rm e}^{\varDelta(\xi_{2k-1},\xi_{2k})}\frac{\rho^{2k}}{\rho^2-1} + \\ & \frac{L_2}{L_1}\frac{\rho^{2k-1}}{\rho^2-1} + \frac{L_4}{L_3}\frac{\rho^{2k}}{\rho^2-1} - \frac{L_4}{L_3}, \end{aligned} \tag{32}$$

其中$\varDelta(\xi_l,\xi_k)$定义为: 对任意的$0\leqslant l<k$,

$$\varDelta(\xi_l,\xi_k) = -L_1\mathcal{T}_{\rm m}(\xi_l,\xi_k) + L_3\mathcal{T}_{\rm p}(\xi_l,\xi_k), \tag{33}$$

这里, $\mathcal{T}_{\rm m}(\xi_l,\xi_k)$表示在时间区间$[\xi_l,\xi_k)$上生成树保持型通信拓扑所占时间, 因此有$\mathcal{T}_{\rm m}(\xi_l,\xi_k) = \xi_k-\xi_l-\mathcal{T}_{\rm p}(\xi_l,\xi_k)$.

对式(32)逐项进行分析. 对于第1项, 根据式(33)和定理中的条件(30), 可知

$$\rho^{2k-1}{\rm e}^{\varDelta(\xi_0,\xi_{2k})} < \frac{1}{\rho}{\rm e}^{-\mu(\xi_{2k}-\xi_0)}, \tag{34}$$

第2项和第1项类似.

对于第3项, 根据式(19)(25), $\mathcal{F}_{\rm p}$的定义以及定理中的条件(30), 可知

$$L_2{\rm e}^{\varDelta(\xi_{2k-1},\xi_{2k})}\rho^{2k}\leqslant \gamma_1{\rm e}^{-\varsigma(\xi_{2k}-\xi_0)}, \tag{35}$$

第4项和第3项类似.

对于第5项, 根据式(35), 显然有

$$L_2\rho^{2k} < \gamma_1{\rm e}^{-\varsigma(\xi_{2k}-\xi_0)}. \tag{36}$$

第6项和第5项类似.

现在分析式(32). 根据式(19)(27)(34)–(36), 可知当$k\to 0$时, $V(\xi_{2k}^-)$以指数收敛到零. 由于序列$\{\xi_{2k}\}$是最恶劣情况, 因此有χ指数收敛到零, 即式(31)成立.

证毕.

3.2 基于障碍李雅普诺夫函数的状态受限控制律设计

第3.1节中, 本文提出了一种分布式的领导车状态观测器. 理论分析表明, 在DoS攻击满足一定约束的前提下, 领导车状态观测器的跟踪误差指数收敛到零, 即存在正常数$\varUpsilon_1$和$\varUpsilon_2$, 使得

$$\| \chi(t) \| \leqslant \varUpsilon_1 \mathrm{e}^{-\varUpsilon_2 t} \| \chi(0) \|,$$

因此, 对所有跟随车i, 在任意时刻$t>0$, 领导车的估计误差始终满足

$$\| \zeta_i(t) - x_0(t) \| \leqslant \| \chi(t) \| < \varUpsilon_1 \| \chi(0) \|, \tag{37}$$

基于这个事实, 当初始估计误差较小时, 可以认为领导车的估计值$\zeta_i = [\zeta_{i,1}\ \ \zeta_{i,2}\ \ \zeta_{i,3}]^{\mathrm{T}}$就代表领导车的状态. 于是对每个跟随车$i$, 根据编队控制的目标, 设计如下参考曲线:

$$y_{i,1}^{\mathrm{r}} = \zeta_{i,1} - i \times d \approx s_0 - i \times d, \tag{38}$$

$$\dot{y}_{i,1}^{\mathrm{r}} = \zeta_{i,2} \approx v_0, \tag{39}$$

$$\ddot{y}_{i,1}^{\mathrm{r}} = \zeta_{i,3} \approx a_0, \tag{40}$$

其中s_0, v_0和a_0分别为领导车的位置、速度和加速度. 如果能设计控制律确保每个跟随车的位置$y_{i,1}$始终满足

$$|y_{i,1} - y_{i,1}^{\mathrm{r}}| < k_{\mathrm{b}1}, \tag{41}$$

那么就可以避免相邻列车发生碰撞, 其中$k_{\mathrm{b}1}$为车队跟踪误差的上界, 满足

$$0 < k_{\mathrm{b}1} < \frac{d - 2\varUpsilon_1 \| \chi(0) \| - \Delta S}{2}. \tag{42}$$

式(41)属于状态受限控制问题的范畴. 此处利用障碍李雅普诺夫函数(barrier Lyapunov function, BLF)[18–19]求解该状态受限控制问题.

下面给出基于BLF的状态受限控制律的具体设计过程. 在式(1a)和式(1b)中, 定义$x_{i,1} = s_i$和$x_{i,2} = v_i$. 同时, 定义输出$y_{i,1} = s_i$和$y_{i,2} = v_i$. 第1步, 针对式(1a), 选择$x_{i,2}$为控制输入, 控制目标是确保列车i的位置$x_{i,1}$跟踪式(38)定义的位置参考曲线$y_{i,1}^{\mathrm{r}}$, 同时确保两者之间的偏差始终满足一个给定的约束$k_{\mathrm{b}1}$. 由于$x_{i,2}$并不是真实的控制输入, 此时设计的控制律称为虚拟控制量.

定义跟随车i的位置跟踪误差如下:

$$e_{i,1} = y_{i,1} - y_{i,1}^{\mathrm{r}} = x_{i,1} - y_{i,1}^{\mathrm{r}}, \tag{43}$$

其中$y_{i,1}^{\mathrm{r}}$为跟随车i的位置参考曲线, 定义见式(38). 对$e_{i,1}$求导数, 并利用式(1a)和式(39), 得

$$\dot{e}_{i,1} = x_{i,2} - \zeta_{i,2} = x_{i,2}^{d} - \zeta_{i,2} + e_{i,2}, \tag{44}$$

其中: $x_{i,2}^{\mathrm{d}}$为虚拟速度控制量, 即期望的速度; $e_{i,2}$为列车i的速度与期望的速度之间的偏差, 定义如下:

$$e_{i,2} = x_{i,2} - x_{i,2}^{\mathrm{d}}, \tag{45}$$

为了确保跟随车i的位置跟踪误差$e_{i,1}$始终满足约束$k_{\mathrm{b}1}$, 定义障碍李雅普诺夫函数为

$$W_{i,1} = \frac{1}{2} \ln \frac{k_{\mathrm{b}1}^2}{k_{\mathrm{b}1}^2 - e_{i,1}^2}, \tag{46}$$

对$W_{i,1}$求导, 并利用式(44), 得

$$\dot{W}_{i,1} = \frac{e_{i,1}}{k_{\mathrm{b}1}^2 - e_{i,1}^2} \left(x_{i,2}^{\mathrm{d}} - \zeta_{i,2} \right) + \frac{e_{i,1} e_{i,2}}{k_{\mathrm{b}1}^2 - e_{i,1}^2},$$

设计虚拟速度控制量$x_{i,2}^{\mathrm{d}}$如下:

$$x_{i,2}^{\mathrm{d}} = -k_1 e_{i,1} + \zeta_{i,2}, \tag{47}$$

其中k_1为控制参数, $k_1 > 0$. 将式(47)代入$W_{i,1}$的导数中, 得

$$\dot{W}_{i,1} = \frac{-k_1 e_{i,1}^2}{k_{\mathrm{b}1}^2 - e_{i,1}^2} + \frac{e_{i,1} e_{i,2}}{k_{\mathrm{b}1}^2 - e_{i,1}^2}, \tag{48}$$

其中等式右边第2项为耦合项, 将在下一步被抵消.

第2步, 基于式(1b)–(1c), 设计最终的控制律u_i, 确保列车i的速度与期望的速度之间的偏差$e_{i,2}$收敛到零, 同时将式(48)中等式右边第2项对应的耦合项抵消掉. 由于执行机构动力学响应带宽远高于控制器带宽, 实际控制器设计时常常忽略执行机构动力学式(1c), 因此式(1b)–(1c)简化为

$$\dot{x}_{i,2} = u_i. \tag{49}$$

对式(45)中的$e_{i,2}$求导数, 根据式(40)(44)(47)(49), 有

$$\dot{e}_{i,2} = u_i + k_1 \left(-k_1 e_{i,1} + e_{i,2} \right) - \zeta_{i,3}, \tag{50}$$

定义李雅普诺夫函数为

$$W_{i,2} = W_{i,1} + \frac{1}{2} e_{i,2}^2, \tag{51}$$

对$W_{i,2}$求导, 并利用式(48)(50), 得

$$\begin{aligned}\dot{W}_{i,2} = {} & \frac{-k_1 e_{i,1}^2}{k_{\mathrm{b}1}^2 - e_{i,1}^2} + \frac{e_{i,1} e_{i,2}}{k_{\mathrm{b}1}^2 - e_{i,1}^2} + \\ & e_{i,2}(u_i + k_1(-k_1 e_{i,1} + e_{i,2}) - \zeta_{i,3}).\end{aligned}$$

因此, 设计最终的控制律如下:

$$\begin{aligned}u_i = {} & -k_2 e_{i,2} - k_1 \left(-k_1 e_{i,1} + e_{i,2} \right) + \zeta_{i,3} - \\ & \frac{e_{i,1}}{k_{\mathrm{b}1}^2 - e_{i,1}^2},\end{aligned} \tag{52}$$

其中k_2为控制器参数, $k_2 > 0$. 将式(52)代入$\dot{W}_{i,2}$的表达式中, 得

$$\dot{W}_{i,2} = -\frac{k_1 e_{i,1}^2}{k_{\mathrm{b}1}^2 - e_{i,1}^2} - k_2 e_{i,2}^2, \tag{53}$$

下面的定理给出了本文提出的弹性控制方法的理论分析结果.

定理 2 假设定理1的所有条件满足. 如果领导车状态观测器的初始估计误差$\chi(0)$满足

$$\parallel \chi(0) \parallel < \frac{d-\Delta S}{2\varUpsilon_1}. \tag{54}$$

同时, 控制律(52)中的控制参数$k_1>0, k_2>0$, 并且k_{b1}满足式(42), 那么, 在控制律(52)下, 系统有如下特性:

1) 碰撞避免满足, 即对所有跟随车i, 当初始时刻控制器的跟踪误差$(e_{i,1}(0), e_{i,2}(0)) \in \varOmega$时, 对所有时刻$t>0$, 有$(e_{i,1}(t), e_{i,2}(t)) \in \varOmega$, 这里, 集合$\varOmega$定义如下:

$$\varOmega = \{(e_{i,1}, e_{i,2}) \big| \, |e_{i,1}| < k_{b1}\}. \tag{55}$$

2) 编队控制满足, 即对所有跟随车i, 当初始时刻控制器的跟踪误差$(e_{i,1}(0), e_{i,2}(0)) \in \varOmega$时, 有$s_{i-1}-s_i-d \to 0, v_i - v_0 \to 0$. 式(54)中, ΔS, d, χ和$\varUpsilon_1$分别在式(10a)、式(10b)、式(15)和式(31)中定义.

证 1) 碰撞避免的证明. 根据$W_{i,1}$的定义式(46), $W_{i,2}$的定义式(51), 以及$W_{i,2}$的导数式(53), 可知在式(55)定义的集合$\varOmega$上, $W_{i,2}$是正定的, $\dot W_{i,2}$是负定的. 于是$W_{i,2}$有界. 因此, 当初始状态位于该集合内, 就始终满足该约束. 根据前面关于碰撞避免的分析, 见式(41)–(42), 可知此时可以避免列车碰撞.

2) 编队控制的证明. 根据$W_{i,1}$的定义式(46), $W_{i,2}$的定义式(51)以及$W_{i,2}$的导数式(53), 应用拉塞尔不变性原理[20], 可知$e_{i,1} \to 0$和$e_{i,2} \to 0$. 根据$e_{i,1}$的定义式(43)和$y^{\rm r}_{i,1}$的定义式(38), 可知列车i的位置满足$s_i = x_{i,1} \to \zeta_{i,1} - i \times d$. 同时, 结合$e_{i,2}$的定义式(45)和$x^d_{i,2}$的定义式(47), 可知列车$i$的速度满足$v_i = x_{i,2} \to \zeta_{i,2}$. 此时, 利用定理1给出的结论$\parallel \chi(t) \parallel \leqslant \varUpsilon_1 {\rm e}^{-\varUpsilon_2 t} \parallel \chi(0) \parallel$并结合跟随车$i$对领导车的状态估计误差$\chi_i$的定义式(16), 可知编队误差满足$s_{i-1}-s_i-d = e_{i-1,1} - e_{i,1} + \chi_{i-1,1} - \chi_{i,1} \to 0$, $v_i - v_0 = v_i - \zeta_{i,2} + \chi_{i,2} \to 0$. 证毕.

4 数学仿真

本节通过一个例子验证本文所提方法的有效性. 首先, 给出仿真中的参数配置情况, 然后, 对仿真结果进行详细介绍.

4.1 仿真参数配置

本文参考了北京地铁7号线仿真平台的相关参数, 如表1所示. 除领导车外, 跟随车有7辆. 在车队控制目标中, 期望间隔d按照下式进行设计:

$$d = \frac{v^2_{\max}}{2u_{\max}} + \Delta S + L.$$

根据表1, 计算得到$d=393$ m.

仿真中, 车车通信拓扑未受到攻击时假设为双前车–跟随车(two-predecessor following, TPF)型拓扑[21], 即每个列车只能收到它的前车和前前车的状态. 领导车的初始位置为0 m, 初始速度为20 m/s. 它的参考曲线$y_{\rm r}$满足$y_{\rm r}(0)=0$, $\dot y_{\rm r}(0) = 20$ m/s, $\ddot y_{\rm r}$满足

$$\ddot y_{\rm r}(t) = \begin{cases} -\dfrac{1}{8}, & 150 < t \leqslant 230, \\ \dfrac{1}{8}, & 340 < t \leqslant 420, \\ 0, & \text{其他}, \end{cases} \tag{56}$$

因此, 仿真中领导车包含了5个阶段, 涉及3次匀速和加减速各一次.

表 1 仿真参数

Table 1 Simulation parameters

参数	符号	值	单位
列车长度	L	118	m
最大速度	$v_{\max}$	30	m/s
最大控制量	$u_{\max}$	2	m/s^2
最小安全距离	ΔS	50	m

进一步, 跟随车i的初始位置为$s_i(0) = s_0(0) - i \times d - 5 \times {\rm rand}$, $v_i(0) = v_0(0) + dv(i)$ 以及$a_i(0)=0$, 这里符号“rand”表示在[0,1]服从均匀分布的随机变量, dv设置为$dv = [6 \;\; 3 \;\; -2 \;\; 2.5 \;\; -5 \;\; 3.5 \;\; 4.2]$m/s.

仿真中, 在式(56)的5个阶段, 共施加了7次DoS攻击, 如图1所示. 发生时间分别为[70, 130] s, [170, 225] s, [260, 293] s, [300, 335] s, [350, 375] s, [382 410] s以及[430, 460] s. 其中, 第1次攻击导致4车收不到3车的消息, 第2次攻击导致1车无法发送和接收消息, 第3次攻击导致3车无法发送和接收消息, 第4次攻击导致2车无法发送和接收消息, 第5次攻击导致5车无法发送和接收消息, 第6次攻击导致3车无法发送和接收消息, 第7次攻击导致6车无法发送和接收消息.

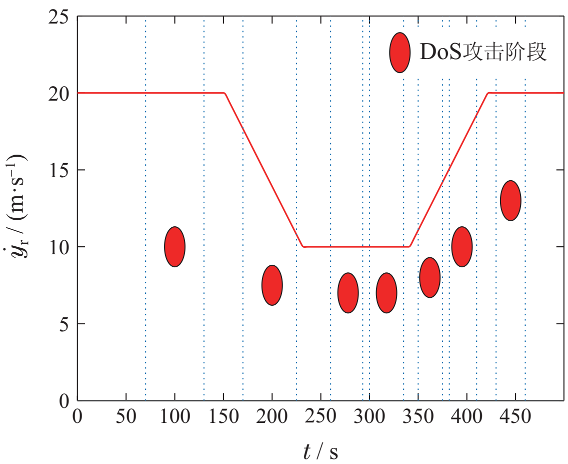

图 1 DoS攻击示意图

Fig. 1 A schematic diagram of DoS attacks

式(2)所示的领导车控制器中, 选取$k_{0,1} = 0.1$, $k_{0,2} = 0.4471$. 式(13)所示的领导车观测器中, 选取

$\varphi = 0.5$. 式(52)所示的基于障碍李雅普诺夫函数的控制器中, 选取$k_{\mathrm{b}1} = 100$, $k_1 = 0.2$, $k_2 = 0.1$. 同时, 选取基于“撞硬墙”防护策略的车队控制方法作为本文的对比方法[22–23].

4.2 仿真结果评价

仿真结果如图2–8所示. 图2给出了领导车状态观测器的位置估计误差. 由图可以看出, 在整个过程中, 即使包含较长时间的DoS攻击, 领导车状态观测器的位置估计仍然具有较好的性能, 位置估计误差最大值不超过5 m. DoS攻击消失时, 位置估计误差快速收敛到零.

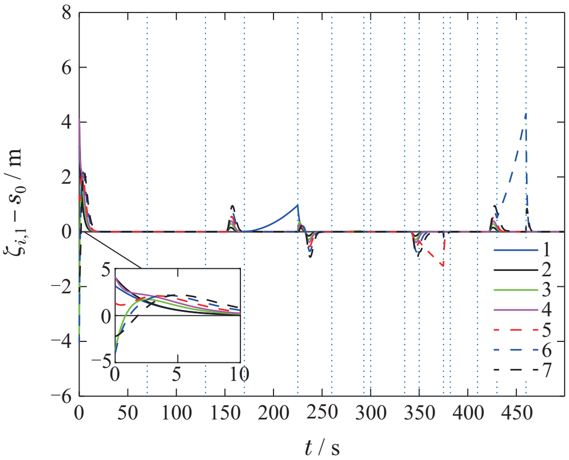

图 2 领导车观测器位置估计误差

Fig. 2 Leader position estimation errors of all the trains

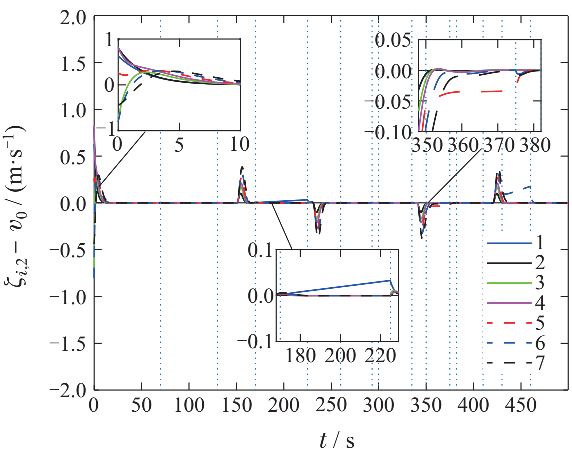

图 3 领导车观测器速度估计误差

Fig. 3 Leader velocity estimation errors of all the trains

图3为领导车状态观测器的速度估计误差曲线. 由图可以看出, 即使存在较长时间的DoS攻击, 整个过程中领导车状态观测器的速度估计具有较好的性能. 本仿真工况下, 速度估计误差最大值不超过1 m/s, 而且最大值是由于初始误差导致的. DoS攻击消失时, 速度估计误差快速收敛到零.

图4为领导车状态观测器的加速度估计误差曲线. 由图可以看出, 整个过程中, 领导车状态观测器的加速度估计具有较好的性能. 本仿真工况下, 加速度估计误差的最大值不超过0.2 m/s^2, 而且最大值出现在式(56)所给的5个阶段的切换时刻. 结合图2–3可知, 和领导车状态观测器的位置估计、速度估计相比, DoS攻击对加速度估计的影响更小.

结合图4的子图可以看出, DoS攻击下, 被攻击列车的加速度估计误差存在常值偏差.

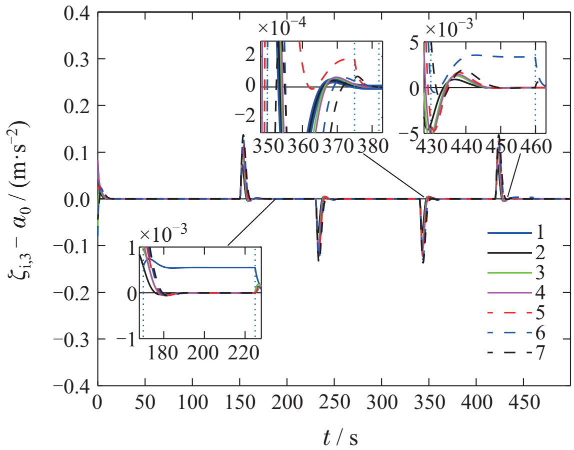

图 4 领导车观测器加速度估计误差

Fig. 4 Leader acceleration estimation errors of all the trains

图5给出了整个过程中的速度编队误差曲线. 由图可以看出, 即使存在较长时间的攻击, 整个过程中列车速度保持的较为一致. 本仿真工况下, 速度编队误差最大值不超过6.1 m/s, 主要是初始误差引起的.

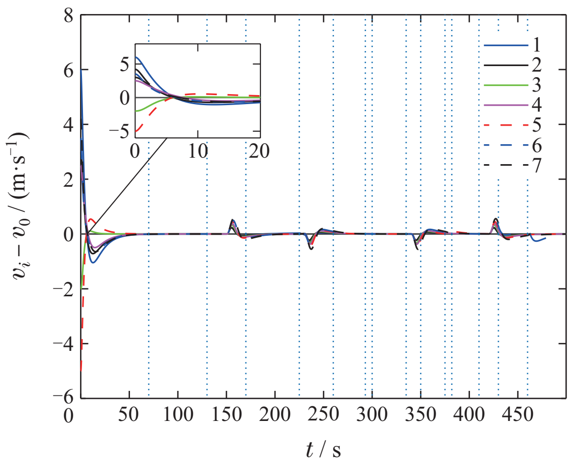

图 5 车队速度跟踪误差

Fig. 5 Platoon velocity tracking errors of all the trains

图6是车队位置跟踪误差曲线. 由图可以看出, 即使存在较长时间的攻击, 车队控制仍然具有较好的性能, 当DoS攻击消失时, 车队位置跟踪误差逐渐趋近于零. 本仿真工况下, 车队位置跟踪误差最大值不超过22 m, 主要是存在初始误差导致的. 根据式(10a)和表1, 可知整个过程中列车未发生碰撞.

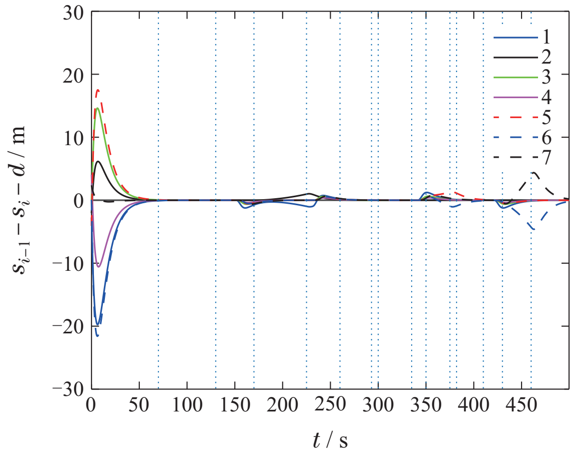

图 6　车队位置跟踪误差

Fig. 6　Platoon position tracking errors of all the trains

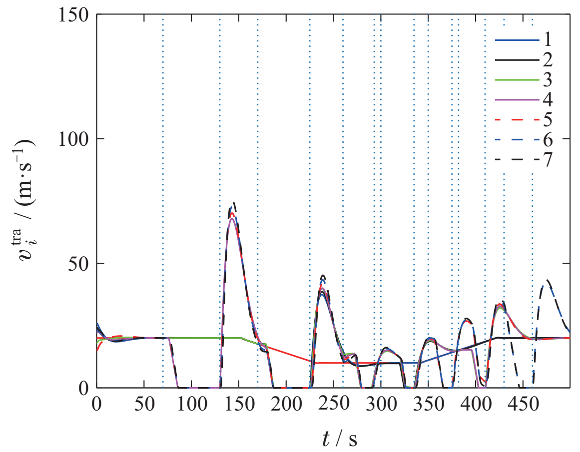

图 7　传统策略下的列车速度

Fig. 7　Velocity of all the trains under the traditional policy

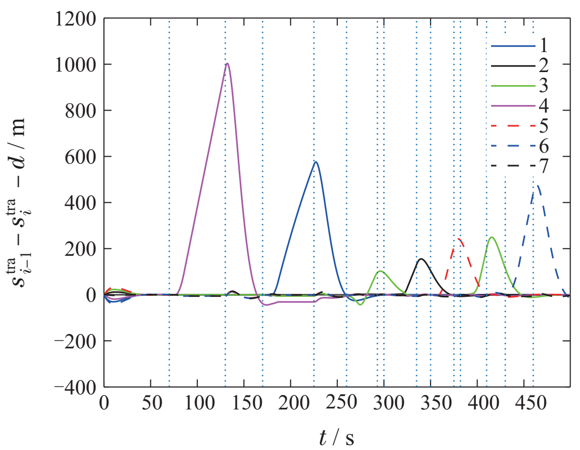

图 8　传统策略下的车队位置跟踪误差

Fig. 8　Platoon position tracking errors of all the trains under the traditional policy

对比方法的列车速度和车队位置跟踪误差分别如图7和图8所示. 由图7可以看出, 在DoS攻击下, 被攻击列车无法接收其他列车的消息, 触发了“撞硬墙”防护策略. 本仿真工况下, 由于DoS攻击时间较长, 触发了紧急制动, 直至停车. 结合图8可知, 由于触发紧急制动, 被攻击列车与前车的距离逐渐扩大, 攻击消失时逐渐恢复到车队控制状态.

上述仿真结果表明, 在较长时间DoS攻击下, 本文提出的弹性控制方法确保了列车始终保持安全距离, 未发生碰撞. 同时, 实现了编队控制的目标. 和现有方法相比, 本文提出的弹性控制方法避免了频繁的紧急制动停车, 提高了运行效率.

5　结论

针对DoS攻击下城市轨道交通列车运行控制系统的弹性控制问题, 本文提出了一种基于领导者状态观测器和障碍李雅普诺夫函数的列车车队弹性控制策略. 理论分析与仿真结果显示, 分布式领导车状态观测器的估计是准确的, 基于障碍李雅普诺夫函数的控制策略有效避免了列车碰撞问题, 同时实现了列车的车队控制问题. 此方法对恶意DoS攻击的效果是显著的, 避免了目前普遍使用的列车“撞硬墙”控制方法引起的列车频繁触发自动防护曲线所导致的紧急制动停车. 同时, 有效提高了列车运行效率, 对城市轨道交通智能等级的有效提升奠定了基础.

参考文献:

[1] GAO B, BU B, ZHANG W, et al. An intrusion detection method based on machine learning and state observer for train-ground communication systems. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 23(7): 6608 – 6620.

[2] GAO B, BU B. A novel intrusion detection method in train-ground communication system. *IEEE Access*, 2019, 7: 178726 – 178743.

[3] MA Jing, YE Yong, JIA Qiusheng. Review of resilient control. *Information and Control*, 2015, 44(1): 67 – 75.
(马静, 叶泳, 贾秋生. 弹性控制综述. 信息与控制, 2015, 44(1): 67 – 75.)

[4] PETRILLO A, PESCAPE A, SANTINI S. A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. *IEEE Transactions on Cybernetics*, 2020, 51(3): 1134 – 1149.

[5] LI Yongfu, WU Changqiang, ZHU Hao, et al. Trajectory tracking control for connected vehicle platoon considering car-following interactions and time delays. *Acta Automatica Sinica*, 2021, 47(9): 2264 – 2275.
(李永福, 邬昌强, 朱浩, 等. 考虑车辆跟驰作用和通信时延的网联车辆队列轨迹跟踪控制. 自动化学报, 2021, 47(9): 2264 – 2275.)

[6] JIN X, HADDAD W M, JIANG Z P, et al. Adaptive control for mitigating sensor and actuator attacks in connected autonomous vehicle platoons. *Conference on Decision and Control (CDC)*. New York: IEEE, 2018: 2810 – 2815.

[7] BIRON Z A, DEY S, PISU P. Resilient control strategy under denial of service in connected vehicles. *American Control Conference (ACC)*. New York: IEEE, 2017: 4971 – 4976.

[8] MERCO R, FERRANTE F, PISU P. A hybrid controller for DoS-resilient string-stable vehicle platoons. *IEEE Transactions on Intelligent Transportation Systems*, 2020, 22(3): 1697 – 1707.

[9] LI Z, LI Z, LIU Y. Resilient control design of the third-order discrete-time connected vehicle systems against cyber-attacks. *IEEE Access*, 2020, 8: 157470 – 157481.

[10] XIAO S, GE X, HAN Q L, et al. Resilient distributed event-triggered control of vehicle platooning under DoS attacks. *IFAC-PapersOnLine*, 2020, 53(2): 1807 – 1812.

[11] KAFASH S H, GIRALDO J, MURGUIA C, et al. Constraining attacker capabilities through actuator saturation. *Annual American Control Conference (ACC)*. New York: IEEE, 2018: 986 – 991.

[12] KEIJZER T, FERRARI R M G. A sliding mode observer approach for attack detection and estimation in autonomous vehicle platoons using event triggered communication. *The 58th Conference on Decision and Control (CDC)*. New York: IEEE, 2019: 5742 – 5747.

[13] ALIPOUR-FANID A, DABAGHCHIAN M, ZENG K. Impact of jamming attacks on vehicular cooperative adaptive cruise control systems. *IEEE Transactions on Vehicular Technology*, 2020, 69(11): 12679 – 12693.

[14] ZHAO Y, LIU Z, WONG W S. Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances. *IEEE Transactions on Intelligent Transportation Systems*, 2021, 23(8): 10945 – 10956.

[15] SU Y, HUANG J. Cooperative output regulation of linear multi-agent systems. *IEEE Transactions on Automatic Control*, 2011, 57(4): 1062 – 1066.

[16] WEN G, DUAN Z, REN W, et al. Distributed consensus of multi-agent systems with general linear node dynamics and intermittent communications. *International Journal of Robust and Nonlinear Control*, 2014, 24(16): 2438 – 2457.

[17] HASSAN K. KHALIL. *Nonlinear Systems*. New York: Prentice Hall, 2002.

[18] JIN X, KWONG R H S. Adaptive fault tolerant control for a class of MIMO nonlinear systems with input and state constraints. *American Control Conference (ACC)*. New York: IEEE, 2015: 2254 – 2259.

[19] SU Z, LI C, WANG H. Barrier Lyapunov function-based robust flight control for the ultra-low altitude airdrop under airflow disturbances. *Aerospace Science and Technology*, 2019, 84: 375 – 386.

[20] SLOTINE J J E, LI W. *Applied Nonlinear Control*. Englewood Cliffs, NJ: Prentice hall, 1991.

[21] ZHENG Y, LI S E, LI K, et al. Distributed model predictive control for heterogeneous vehicle platoons under unidirectional topologies. *IEEE Transactions on Control Systems Technology*, 2016, 25(3): 899 – 910.

[22] CHEN L, NING B, XU T H. Research on modeling and simulation of vehicle-on-board automatic train protection subsystem of communication based train control system. *International Conference on Vehicular Electronics and Safety*. Beijing: IEEE, 2007: 1 – 5.

[23] NING B, DONG H, GAO S, et al. Distributed cooperative control of multiple high-speed trains under a moving block system by nonlinear mapping-based feedback. *Science China Information Sciences*, 2018, 61(12): 1 – 12.

作者简介:

高 兵 博士研究生, 目前主要研究方向为列车通信安全、列车弹性控制, E-mail: 17111041@bjtu.edu.cn;

步 兵 教授, 博士生导师, 目前研究方向为列车通信安全、列车控制, E-mail: bbu@bjtu.edu.cn.