DoS攻击下基于多率采样的多智能体系统安全一致性

王 悦[1], 贾新春[2†], 游 秀[1], 吕 腾[1]

(1. 山西大学 数学科学学院, 山西 太原 030006; 2. 山西大学 自动化与软件学院, 山西 太原 030013)

摘要: 本文研究了一类带有多率采样的线性多智能体系统(MASs)在拒绝服务(DoS)攻击下的安全一致性控制问题, 其中DoS攻击通常阻断智能体之间的信息传输. 本文将多率采样在网络化控制系统中的结果推广到了多智能体系统, 并考虑了非理想通信网络环境. 首先, 通过引入一个匹配机制来同步由多率采样引起的智能体不同状态分量的采样数据. 然后, 在DoS攻击下, 针对带有多率采样的线性MAS提出了一个基于多率采样的安全一致性控制器. 通过使用李雅普诺夫稳定性理论和切换系统方法, 获得了包含DoS攻击持续时间以及攻击频率的安全一致性充分条件. 最后, 给出了一个仿真例子来验证所提方法的有效性, 并给出了多率采样与单率采样机制的性能对比分析.

关键词: 多智能体系统; 多率采样; 拒绝服务攻击; 安全控制; 一致性控制

引用格式: 王悦, 贾新春, 游秀, 等. DoS攻击下基于多率采样的多智能体系统安全一致性. 控制理论与应用, 2022, 39(10): 1890 – 1897

DOI: 10.7641/CTA.2022.10985

Multi-rate sampled-data secure consensus of multi-agent systems subject to DoS attacks

WANG Yue[1], JIA Xin-chun[2†], YOU Xiu[1], LÜ Teng[1]

(1. School of Mathematical Sciences, Shanxi University, Taiyuan Shanxi 030006, China;
2. School of Automation and Software Engineering, Shanxi University, Taiyuan Shanxi 030013, China)

Abstract: This paper studies the secure consensus control problem for a class of linear multiagent systems (MASs) with a multi-rate sampling under denial-of-service (DoS) attacks, where DoS attacks usually prevent information transmission among agents. The results of the multi-rate sampling strategy in networked control systems are extended to MASs and a non-ideal communication network is considered in this paper. Firstly, a matching mechanism is introduced in order to synchronize the sampled data of different state components of agents caused by multi-rate sampling. Then, a multi-rate sampling based secure consensus controller is designed for linear MAS with a multi-rate sampling under DoS attacks. By using Lyapunov stability theory and switched system method, a sufficient condition with the DoS attack duration and frequency is obtained. Finally, a simulation example is presented to verify the effectiveness of the proposed method and exhibit the performance comparing analysis between the multi-rate sampling and the single-rate sampling mechanism.

Key words: multi-agent systems (MASs); multi-rate sampling; denial-of-service (DoS) attacks; secure control; consensus control

Citation: WANG Yue, JIA Xinchun, YOU Xiu, et al. Multi-rate sampled-data secure consensus of multi-agent systems subject to DoS attacks. *Control Theory & Applications*, 2022, 39(10): 1890 – 1897

1 引言

近几十年来, 多智能体系统(multi-agent systems, MASs) 的协同控制由于其广泛的应用领域吸引了众多专家学者的关注. 一致性问题作为多智能体系统协同控制领域的一个基本问题, 其控制目标是设计一个合适的控制协议, 在智能体受到共享通信网络资源的限制下, 仍能使所有智能体的状态或者输出收敛到一个常值[1–2]. 而由于通信网络的引入, 诸如通信资源的

收稿日期: 2021−10−16; 录用日期: 2022−03−30.

†通信作者. E-mail: xchjia@sxu.edu.cn; Tel.: +86 35-12646020.

本文责任编委: 朱善迎.

国家自然科学基金项目(61973201, 61803243), 山西省教育厅高校科技创新项目(2020L0011), 博士后创新人才支持计划项目(BX20200201), 中国博士后科学基金第69批面上项目(2021M691988)资助.

Supported by the National Natural Science Foundation of China (61973201, 61803243), the Science Technology Innovation Project of Shanxi Province Department of Education (2020L0011), the Postdoctoral Innovative Talent Support Program of China (BX20200201) and the China Postdoctoral Science Foundation (2021M691988).

消耗和网络攻击的影响等, 给MASs的一致性分析带来巨大的挑战.

大多数现存的文献都集中于基于连续通信的MASs控制研究, 这就意味着智能体需要足够强的计算能力和理想的通信环境, 这对数字网络环境下的MASs来说并不现实. 近年来在网络化控制系统中已有很多关于采样方法的优秀成果, 例如文献[3–5]. 此外, 专家学者们对在采样环境下MASs的研究做出了很多努力[6–9]. 在现存文献中, 采样框架大致分为两类: 同步采样和异步采样. 前者为每一个智能体的状态或输出由不同的传感器节点在同一时刻被采样; 后者则是不同的智能体传感器有不同的采样周期. 例如, 文献[7]和文献[8]分别研究了一类线性MASs在同步采样和异步采样策略下的一致性问题. 文献[9]在此基础上, 分别针对二阶MASs, 在同步非均匀采样与异步非均匀采样策略下, 提出了新颖的基于连续–离散时间观测器的一致性分布式协议. 但是这些采样方法都是基于单率采样策略, 即智能体所有的量测分量都在相同时刻被传感器采集, 这对一些实际的工业应用来说较难实现. 因此, 控制系统的多率采样的策略应运而生.

实际上, 不同类型的传感器组对智能体不同量测分量进行采样时的采样周期一般是不同的. 比如在车辆横向控制中, 往往使用超音速传感器对车辆的位移和速度进行采样, 而对角速度和横摆角的采样则使用陀螺仪传感器[10]. 这是由于智能体不同量测分量的物理特性造成的, 若采用单率采样策略, 对保证系统性能来说具有一定的保守性. 因此, 为了保证系统的实时性并提高数据的利用率, 就有必要研究控制系统的多率采样策略. 此外, 由于多率采样策略下MASs一致性的分析较为复杂, 目前大部分关于多率采样策略的研究局限于网络化控制系统[10–12], 最近, 文献[13]研究了一类异构MASs在多率采样下的输出一致性问题. 然而关于MASs在多率采样下的一致性问题的研究仍然存在一些挑战, 这是本文的主要研究动机之一.

另一方面, 随着网络技术的发展, 网络安全对保证系统性能方面来说至关重要. 严重的网络攻击会破坏系统的控制性能, 甚至导致系统大范围瘫痪. 拒绝服务(denial-of-service, DoS)攻击[14–19]作为一种最常见和最具破坏力的网络攻击之一, 其目的是通过阻止智能体之间的信息传输来破坏系统的稳定性. 文献[16]和文献[17]分别针对受到周期性DoS攻击和一般DoS攻击的MASs的事件触发安全一致性问题进行了研究. 文献[18]进一步考虑了针对多条通信链路独立进行DoS攻击的情况, 提出了一个新颖的分布式安全控制器. 然而, 这些文献中大都采用同步/异步采样策略或者事件触发方法, 为了使MASs在DoS攻击下仍然能够表现出良好的控制性能, 研究此类系统在多率采样策略下的一致性控制问题在理论上具有一定的挑战性. 这是本文的第2个主要研究动机.

受上述研究内容的启发, 本文针对一类带有多率采样的线性MASs, 考虑智能体之间通信链路存在DoS攻击的情况, 运用李雅普诺夫稳定性理论和切换系统理论, 提出一个安全一致性控制器, 实现了MASs的安全一致性控制. 通过为每一个智能体引入一个匹配缓冲器, 解决了由多率采样引起的智能体各采样分量的时序不同步问题, 并且获得了包含DoS攻击持续时间和频率的一致性条件. 本文的主要贡献总结如下:

1) 不同于文献[6–8]采用的单率采样, 本文研究了带有多率采样的MASs的一致性问题, 不仅避免了智能体之间的连续通信, 且提高了数据的实时性和利用率, 使得系统能够更快速地达到一致性;

2) 不同于文献[9–13]和[14–19], 本文同时考虑了多率采样与非理想通信网络环境. 在DoS攻击下, 设计了一种新颖的基于多率采样的安全切换控制器. 在所提控制策略下, MASs能够达到指数一致性.

2 准备工作和问题描述

本文使用标准符号. $\mathbb{R}^n$表示n维欧式空间; $\mathbb{R}^{n\times m}$表示n行m列实矩阵的集合. I_N表示适当维数的单位矩阵; $\mathbf{1}$表示n维全1列向量; $\mathbb{N}_p$表示从1到p的整数集, $\mathbb{N}^+$表示正整数集. diag$\{\cdot\}$为对角矩阵. col$(\cdots)$表示列向量. 对于实对称矩阵P, P^{T}表示矩阵P的转置; $P>0$意味着矩阵P是正定矩阵. 矩阵A和B的克罗内克积记为$A\otimes B$. 对于给定的两个集合Γ_1和Γ_2, $\Gamma_1\backslash\Gamma_2$表示在$\Gamma_1$中$\Gamma_2$的相对补. $\|\cdot\|$表示向量或矩阵的范数. $\lambda_{\max}(A)$和$\lambda_{\min}(A)$分别表示矩阵A的最大和最小特征值.

2.1 代数图论

考虑无向图$\mathcal{G}=\{\mathcal{V},\mathcal{E},\mathcal{A}\}$, 其中$\mathcal{V}=\{v_1,v_2,\cdots,v_N\}$表示节点集, 有限非空集$\mathcal{I}=\{1,2,\cdots,N\}$为节点序号集, 用$\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$表示边集, $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$为图$\mathcal{G}$的邻接矩阵. 当节点$v_i$能够收到$v_j$的信息, 即边$(v_i,v_j)\in\mathcal{E}$时, $a_{ij}=1$; 否则$a_{ij}=0$. 智能体i的邻居集合用N_i表示. 图$\mathcal{G}$的拉普拉斯矩阵为$L=[l_{ij}]$, $l_{ij}=-a_{ij},\forall i\neq j$; $l_{ij}=-a_{ij},\forall i\neq j$; $l_{ii}=\sum\limits_{j=1,j\neq i}^{N}a_{ij}$. 定义$\lambda_1\leqslant\lambda_2\leqslant\cdots\leqslant\lambda_N$为$L$的特征值.

2.2 问题描述

考虑一类带有N个智能体的同构线性多智能体系统. 智能体i $(i=1,2,\cdots,N)$的动力学描述如下:

$$\dot{x}_i(t)=Ax_i(t)+Bu_i(t), \tag{1}$$

其中: $x_i(t)\in\mathbb{R}^n$和$u_i(t)\in\mathbb{R}^m$分别为第i个智能体的状态和控制输入. $A\in\mathbb{R}^{n\times n}$和$B\in\mathbb{R}^{n\times m}$为适当维数的已知常矩阵. 假设矩阵$A$不是赫尔维兹的, 但矩

阵对(A,B)是可镇定的.

此外, 每个智能体i的状态$x_i(t)$由不同传感器组进行多率采样. 假设$x_i(t)$的n个分量被划分为p个子向量, 每一个子向量由相应的传感器组进行采样. 定义$x_i(t)=[x_{i1}^{\mathrm{T}}(t)\ \ x_{i2}^{\mathrm{T}}(t)\ \ \cdots\ \ x_{i\beta}^{\mathrm{T}}(t)\ \ \cdots\ \ x_{ip}^{\mathrm{T}}(t)]^{\mathrm{T}}$, 其中$p\in\mathbb{N}^+, p\leqslant n, \beta\in\mathbb{N}_p$, 即第$\beta$个子向量$x_{i\beta}(t)\in\mathbb{R}^{n_{i\beta}}$由传感器组$S_{i\beta}$以周期$T_{i\beta}$(采样率$f_{i\beta}=1/T_{i\beta}$)采样, 且$n_{i\beta}$满足$\sum\limits_{\beta=1}^{p}n_{i\beta}=n$. 传感器组$S_{i\beta}$的采样序列记为$\{x_{i\beta}(0),x_{i\beta}(T_{i\beta}),x_{i\beta}(2T_{i\beta}),\cdots,x_{i\beta}(k_{i\beta}T_{i\beta}),\cdots\}$, $k_{i\beta}\in\mathbb{N}$. 然后, 基于所提出的多率采样策略, 对于$t\in[k_{i\beta}T_{i\beta},(k_{i\beta}+1)T_{i\beta}], \beta\in\mathbb{N}_p$, 使用零阶保持器(zero-order holder, ZOH)可得到经过多率采样后的状态向量$\tilde{x}_i(t)$的表达式为

$$\tilde{x}_i(t)=\sum_{\beta=1}^{p}D_{i\beta}x_{i\beta}(k_{i\beta}T_{i\beta}),\quad t\in[k_{i\beta}T_{i\beta},(k_{i\beta}+1)T_{i\beta}),\ \beta\in\mathbb{N}_p,\tag{2}$$

其中: $D_{i\beta}=[0_{n_{i\beta}\times l_{i\beta}}\ \ I_{n_{i\beta}}\ \ 0_{n_{i\beta}\times(n-n_{i\beta}-l_{i\beta})}]^{\mathrm{T}}$, $l_{i\beta}=\sum\limits_{v=1}^{\beta-1}n_{iv}$. 特别地, 当$\beta=1$时, 令$l_{i\beta}=0$. 此外, 注意不同的传感器组应有不同的采样周期, 即$T_{i\beta}\neq T_{i\alpha}(\alpha\neq\beta,\ \alpha,\beta\in\mathbb{N}_p)$.

在本文所提出的多率采样策略中, 引入了匹配机制来解决时序不同步问题, 该匹配机制中包含一个匹配缓冲器, 即每个智能体i的状态分量$x_{i\beta}(t)$被相应的传感器组$S_{i\beta}$独立采样并传输到缓冲器buffer$_i$中. buffer$_i$的作用是, 只要有一组传感器将采样得到的数据传输到缓冲器时, 缓冲器就将智能体i的各状态分量组合打包为一个数据包, 将其发送到智能体i的收发器. 然后收发器将这个数据包传输给邻居智能体j. 此时, 在打包传输的状态值中只有一个或几个状态分量得到更新, 其他状态分量仍然使用前一时刻的采样值.

注 1 一般地, 每个智能体配置有多个传感器, 不同物理属性的传感器一般有着不同的有效采样率范围, 它们是由传感器的物理属性决定的, 即多率采样. 为了简化问题, 现有文献大多假设单个智能体内配置的传感器组的采样率f_i是相同的, 即单率采样. 若所有智能体的采样率相同, 即$f_i=f_j$, $i,j\in\mathcal{I}$, 则把这样的采样策略称为同步采样; 若至少有两个智能体的采样率不同, 即$f_i\neq f_j, i,j\in\mathcal{I}$, 则称为异步采样, 详情见文献[13]. 通过设置缓存器使得控制器中数据的更新以所有采样分量的最小公倍周期为公共采样周期, 即所有状态分量采样周期相同时, 多率采样就转化为了单率采样. 因此, 可以把单率采样看作多率采样的特例, 在第4节仿真部分将进行相应对比.

2.3 DoS攻击模型

在本文中, 假设当DoS攻击处于活跃期间时, 智能体之间的信息交换被阻断且通信拓扑为零拓扑. 考虑通信信道(i,j)被阻断时信道(j,i)也被阻断的情况, 即无向通信拓扑. 定义$I_m=[\tilde{t}_m,\tilde{t}_m+\tilde{\tau}_m)$为第$m$次攻击间隔, 其中$m\in\mathbb{N}$. $\tilde{t}_m$和$\tilde{t}_m+\tilde{\tau}_m$分别表示第$m$次DoS攻击的开始时刻和结束时刻, 第$m$次DoS攻击的持续时间为$\tilde{\tau}_m$. 对于任意的$t_2\geqslant t_1$, 定义$\Pi_a(t_1,t_2)\triangleq\bigcup I_m\bigcap(t_1,t_2)$为在时间段$(t_1,t_2)$内攻击者阻塞智能体间通信的时间间隔的集合. 相应地, 令$\Pi_s(t_1,t_2)\triangleq[t_1,t_2]\backslash\Pi_a(t_1,t_2)$为智能体间正常通信的时间间隔的集合.

定义$\sigma(t)$为攻击信号, 当攻击者发动DoS攻击时, $\sigma(t)=0$, 否则$\sigma(t)=1$. 本文使用了攻击确认机制, 通过$\sigma(t)$确定攻击何时开始和结束. 此外, 关于攻击检测算法的研究也越来越多[20]. $\sigma(t)$的数学描述如下:

$$\sigma(t)=\begin{cases}1, & t\in\Pi_s(t_1,t_2),\\ 0, & t\in\Pi_a(t_1,t_2).\end{cases}\tag{3}$$

假设在初始时刻t_0, $\sigma(t_0)=1$.

受平均驻留时间(average dwell time, ADT)概念的启发, 对攻击持续时间和攻击频率做出如下假设:

假设 1 假设初始时刻为t_0, 对于任意的$t>t_0$, 在$[t_0,t)$内DoS攻击的持续时间为$\Pi_a(t_0,t)$. 存在常数$\Pi_0>0$, $1/T\in[0,1)$使得

$$|\Pi_a(t_0,t)|\leqslant\Pi_0+\frac{t-t_0}{T},\tag{4}$$

其中$|\Pi_a(t_0,t)|$和$1/T$分别表示$\Pi_a(t_0,t)$的勒贝格测度和攻击强度.

假设 2 假设初始时刻为t_0, 对于任意的$t>t_0$, 在$[t_0,t)$内DoS攻击的次数定义为$|n(t_0,t)|$. 存在常数$n_0>0$, $\tau_D>0$使得

$$|n(t_0,t)|\leqslant n_0+\frac{t-t_0}{\tau_D}.\tag{5}$$

注 2 假设1和假设2在一些文献中是很标准的假设. 假设1中的标量$1/T$表示在长时间间隔内, 攻击持续时间平均率的上界. 例如, 当$1/T=0.75$时, 总攻击时长不能超过总时间跨度的75%. 如果攻击从$t_0=0$时刻开始, 那么攻击间隔长度的上界就为$\tau\leqslant\Pi_0/(1-1/T)$. 因此, 标量$\Pi_0$可以作为描述攻击者初始能力的参数. 相应地, 式(5)中的标量$1/\tau_D$表示在长时间间隔内攻击频率的上界.

2.4 控制目标

本文的控制目标是, 在存在DoS攻击的情况下, 针对带有多率采样的多智能体系统设计一个合理的安全控制策略, 使得对于任意的初始条件, 智能体的状态满足

$$\lim_{t\to\infty}\Big\|x_i(t)-\frac{1}{N}\sum_{j=1}^{N}x_j(t)\Big\|=0,\tag{6}$$

其中$i,j=1,2,\cdots,N$.

3　主要结论

在本节中, 将提出针对带有多率采样的线性多智能体系统的一个安全控制策略. 通过分析受DoS攻击影响的闭环系统的稳定性, 得到了仍然能够保持一致性性能的关于DoS攻击持续时间和频率的充分条件.

3.1　控制器设计

考虑在DoS攻击下, 带有多率采样的多智能体系统(1), 为每一个智能体i $(i \in \mathcal{I})$设计如下形式的安全控制器:

$$u_i(t) = K\varphi_i(t). \tag{7}$$

其中: $\varphi_i(t)=\sum\limits_{j=1}^{N}a_{ij}\sigma(t)(\hat{x}_j(t)-\hat{x}_i(t))$, $\hat{x}_i(t)=\mathrm{e}^{A(t-t_k^i)}\tilde{x}_i(t_k^i)$为$\tilde{x}_i(t_k^i)$的开环估计, $t\in[t_k^i,t_{k+1}^i)$, $i=1,2,\cdots,N$. 矩阵K 为待设计的控制增益矩阵. $\tilde{x}_i(t_k^i)$为在时刻t_k^i第i个智能体的状态向量, t_k^i为多率采样时刻, 满足

$$t_k^i = \arg\min_{k_{i\beta}T_{i\beta}} \left\{t - k_{i\beta}T_{i\beta} | t \geqslant k_{i\beta}T_{i\beta} > t_{k-1}^i\right\}. \tag{8}$$

其中: $\beta \in \mathbb{N}_p, k \in \mathbb{N}^+$. 多率采样初始时刻$t_i^0 = 0$. 例如, 假设每个智能体有两个状态分量, 各状态分量$x_{i1}(t), x_{i2}(t)(i \in \mathcal{I})$与控制器$u_i(t)$的更新时刻在图1给出.

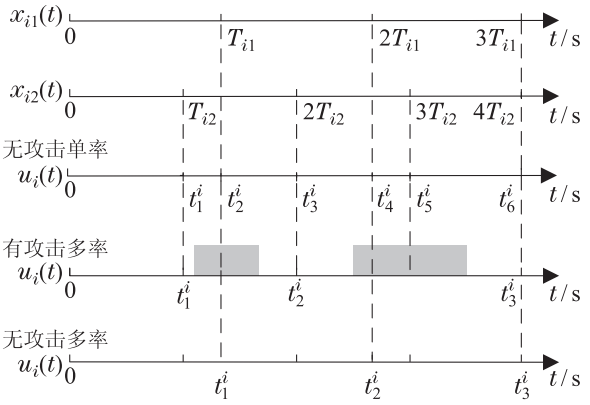

图 1　多率采样时刻及控制器更新时刻

Fig. 1　The multi-rate sampling instants and the controller updated instants

注 3　从图1中可以看出, 在多率采样下, 只要有任一分量更新, 则控制器更新; 而在单率采样下, 控制器需要等待一段时间才能更新, 因此其更新次数明显少于多率采样. 当发生DoS攻击时, 由于控制器收不到来自邻居的信息, 则控制器不更新.

注意到, 联合误差项$\varphi_i(t)$的取值依赖于攻击信号$\sigma(t)$. 当智能体之间进行正常通信时, $\varphi_i(t)=\sum\limits_{j=1}^{N}a_{ij}(t)(\hat{x}_j(t)-\hat{x}_i(t))$; 否则, 当时刻$t\in[t_k^i,t_{k+1}^i)$ 时通信信道被DoS攻击阻断, 则$\varphi_i(t)=0$. 本文的安全控制策略整体框架如图2所示. 图中每个智能体的匹配机制中包含一个缓冲器, 其运行原理已在第1.2 节中详细介绍, 此处不再赘述.

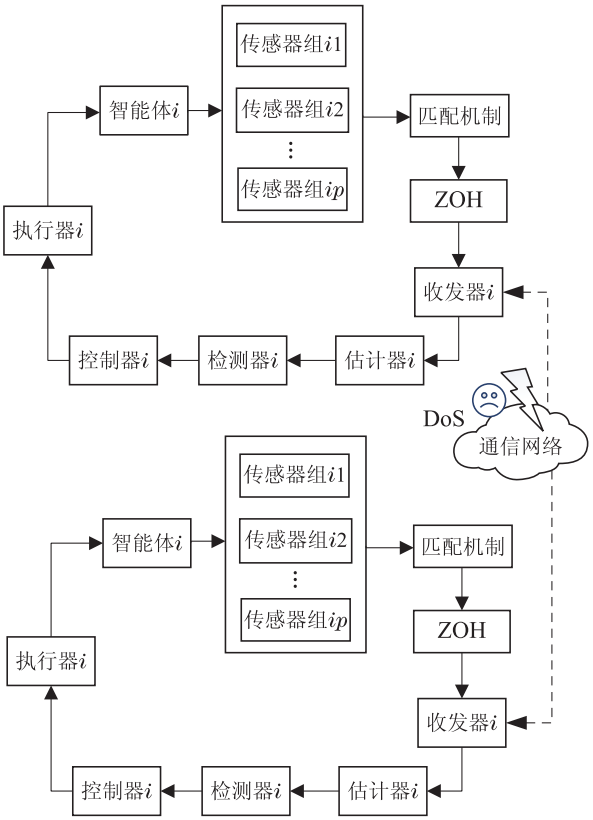

图 2　拒绝服务攻击下带有多率采样的多智能体系统安全控制框架

Fig. 2　The secure control framework of MAS(1) with multi-rate sampling under DoS attacks

3.2　一致性分析

定义一致性误差向量$\varepsilon_i(t) = x_i(t) - \bar{x}(t)$, 其中, $\bar{x}(t) = \dfrac{1}{N}\sum\limits_{j=1}^{N}x_j(t)$. 由此可得增广形式:

$$\varepsilon(t) = (\mathcal{M} \otimes I_n)x(t), \tag{9}$$

其中: $\varepsilon(t)=\mathrm{col}(\varepsilon_1(t),\cdots,\varepsilon_N(t))$, $x(t)=\mathrm{col}(x_1(t),\cdots,x_N(t))$, $\mathcal{M} = I_N - \dfrac{1}{N}\mathbf{1}\mathbf{1}^{\mathrm{T}}$. 定义估计误差向量$\hat{\varepsilon}_i(t) = \hat{x}_i(t) - \dfrac{1}{N}\sum\limits_{j=1}^{N}\hat{x}_j(t)$和测量误差向量$e_i(t) = \hat{\varepsilon}_i(t) - \varepsilon_i(t)$. 为了简化书写, 令

$$\begin{aligned}\varphi(t) &= \mathrm{col}(\varphi_1(t),\cdots,\varphi_N(t)),\\ \mathrm{e}(t) &= \mathrm{col}(e_1(t),\cdots,e_N(t)),\\ \hat{\varepsilon}(t) &= \mathrm{col}(\hat{\varepsilon}_1(t),\cdots,\hat{\varepsilon}_N(t)).\end{aligned}$$

然后, 闭环误差系统可以进一步表示为

$$\dot{\varepsilon}(t) = (I_N \otimes A)\varepsilon(t) + (\mathcal{M} \otimes BK)\varphi(t). \tag{10}$$

容易得到

$$\varphi(t) = \begin{cases} -(L \otimes I_n)\hat{\varepsilon}(t), & t \in \Pi_s(0,\infty),\\ 0, & t \in \Pi_a(0,\infty). \end{cases} \tag{11}$$

令$\delta(t)=[(\varepsilon(t)\ \ e(t))]^{\mathrm{T}}$, 可得

$$\dot{\delta}(t)=\begin{cases}\Lambda_1\delta(t),\ \ t\in\Pi_s(0,\infty),\\ \Lambda_2\delta(t),\ \ t\in\Pi_a(0,\infty),\end{cases}\tag{12}$$

其中:

$$\Lambda_1=\begin{bmatrix}I_N\otimes A-L\otimes BK & -L\otimes BK\\ L\otimes BK & I_N\otimes A+L\otimes BK\end{bmatrix},$$

$$\Lambda_2=\begin{bmatrix}I_N\otimes A & 0\\ 0 & I_N\otimes A\end{bmatrix}.$$

在给出主要结论之前, 为了书写简便, 引入一些符号. 令

$$\begin{cases}\lambda_m &=\lambda_{\min}(P),\\ \lambda_M &=\lambda_{\max}(P),\\ c_1 &=2\left\|L\right\|\left\|PBK\right\|,\\ \alpha_1 &=\dfrac{\lambda_M\mu_1-2c_1}{\lambda_m},\\ \alpha_2 &=\dfrac{\lambda_M\mu_2}{\lambda_m}.\end{cases}\tag{13}$$

定理 1 考虑无向连通图$\mathcal{G}$, 在DoS攻击满足假设1和假设2的条件下, 带有多率采样的多智能体系统(1)在设计的控制协议(7)控制下, 对于给定的常数$\mu_1>0$, $\mu_2>0$, 如果存在矩阵$P>0$使得下列黎卡提不等式成立:

$$PA+A^{\mathrm{T}}P-\frac{1}{2\lambda_2(L)}PBB^{\mathrm{T}}P+\mu_1P<0,\tag{14}$$

$$PA+A^{\mathrm{T}}P-\mu_2P<0,\tag{15}$$

并且满足

$$\frac{\alpha_1}{\alpha_1+\alpha_2}>\frac{\tau_D+\tau T}{\tau_D T},\tag{16}$$

则称带有多率采样(8)的多智能体系统(1)在受到DoS攻击影响下仍然能够达到一致性, 且控制增益矩阵$K=B^{\mathrm{T}}P$.

证 考虑如下李雅普诺夫函数:

$$V(t)=\delta^{\mathrm{T}}(t)\Omega\delta(t),\tag{17}$$

其中$\Omega=\mathrm{diag}\{I_N\otimes P,\ I_N\otimes P\}$.

情况 1 多智能体系统(1)没有受到DoS攻击. 显然, 当$t\in\Pi_s(0,\infty)$时, 从式(17)可以得到

$$\begin{aligned}\dot{V}(t)=&2\varepsilon^{\mathrm{T}}(t)(I_N\otimes P)\dot{\varepsilon}(t)+2e^{\mathrm{T}}(t)(I_N\otimes P)\dot{e}(t)=\\ &2\varepsilon^{\mathrm{T}}(t)(I_N\otimes P)[(I_N\otimes A-L\otimes BK)\varepsilon(t)-\\ &(L\otimes BK)e(t)]+2e^{\mathrm{T}}(t)(I_N\otimes P)[(I_N\otimes\\ &A+L\otimes BK)e(t)+(L\otimes BK)\varepsilon(t)]=\\ &\varepsilon^{\mathrm{T}}(t)\left[I_N\otimes(PA+A^{\mathrm{T}}P)-2L\otimes PBK\right]\times\\ &\varepsilon(t)-2\varepsilon^{\mathrm{T}}(t)\left(L\otimes PBK\right)e(t)+e^{\mathrm{T}}(t)\left[I_N\otimes\right.\\ &\left.(PA+A^{\mathrm{T}}P)-2L\otimes PBK\right]e(t)+2e^{\mathrm{T}}(t)\times\\ &(2L\otimes PBK)e(t)+2e^{\mathrm{T}}(t)(L\otimes PBK)\varepsilon(t).\end{aligned}$$

基于式(14)和杨氏不等式, 可以推出

$$\begin{aligned}\dot{V}(t)\leqslant&-\varepsilon^{\mathrm{T}}(t)\left(I_N\otimes\mu_1P\right)\varepsilon(t)-\\ &e^{\mathrm{T}}(t)(I_N\otimes\mu_1P)e(t)+\\ &2e^{\mathrm{T}}(t)\left(2L\otimes PBK\right)e(t)\leqslant\\ &-\lambda_M\mu_1\|\varepsilon(t)\|^2-\lambda_M\mu_1\|e(t)\|^2+\\ &2c_1\|e(t)\|^2\leqslant\\ &-(\lambda_M\mu_1-2c_1)(\|\varepsilon(t)\|^2+\|e(t)\|^2)\leqslant\\ &-\frac{\lambda_M\mu_1-2c_1}{\lambda_m}V(t)=-\alpha_1V(t).\end{aligned}$$

因此, 对于$t\in\Pi_s(0,\infty)$可得

$$\dot{V}(t)\leqslant-\alpha_1V(t).\tag{18}$$

情况 2 多智能体系统(1)受到DoS攻击.

$$\begin{aligned}&\dot{V}(t)=\\ &2\varepsilon^{\mathrm{T}}(t)(I_N\otimes P)\dot{\varepsilon}(t)+2e^{\mathrm{T}}(t)(I_N\otimes P)\dot{e}(t)=\\ &2\varepsilon^{\mathrm{T}}(t)(I_N\otimes P)(I_N\otimes A)\varepsilon(t)+2e^{\mathrm{T}}(t)\times\\ &(I_N\otimes P)(I_N\otimes A)e(t)=\\ &\varepsilon^{\mathrm{T}}(t)[I_N\otimes(PA+A^{\mathrm{T}}P)]\varepsilon(t)+\\ &e^{\mathrm{T}}(t)[I_N\otimes(PA+A^{\mathrm{T}}P)]e(t).\end{aligned}$$

基于式(15), 有

$$\begin{aligned}\dot{V}(t)\leqslant&\ \varepsilon^{\mathrm{T}}(t)(I_N\otimes\mu_2P)\varepsilon(t)+\\ &e^{\mathrm{T}}(t)(I_N\otimes\mu_2P)e(t)\leqslant\\ &\lambda_M\mu_2(\|\varepsilon(t)\|^2+\|e(t)\|^2)\leqslant\\ &\frac{\lambda_M\mu_2}{\lambda_m}V(t)=\alpha_2V(t).\end{aligned}$$

因此, 对于$t\in\Pi_a(0,\infty)$, 不难得到

$$\dot{V}(t)\leqslant\alpha_2V(t).\tag{19}$$

综上, 从上述分析中可得

$$\dot{V}(t)\leqslant\begin{cases}-\alpha_1V(t),\ \ t\in\Pi_s(0,\infty),\\ \alpha_2V(t),\ \ \ \ t\in\Pi_a(0,\infty).\end{cases}\tag{20}$$

若DoS攻击发生在两次采样时刻之间, 则认为是无效的DoS攻击, 即智能体仍然保持正常通信; 如果攻击在某一个采样时刻之前结束, 则将DoS攻击结束时刻到该采样时刻之间恢复通信的时间记作τ. 因此, 为了书写简便, 重新定义$[\tilde{t}_m,\tilde{t}_m+\tilde{\tau}_m+\tau)$为第$m$次攻击间隔, $[\tilde{t}_m+\tilde{\tau}_m+\tau,\tilde{t}_{m+1})$为正常通信的时间间隔. 进一步地, 定义$\tilde{\Pi}_a(t_0,t)=\bigcup\limits_m[\tilde{t}_m,\tilde{t}_m+\tilde{\tau}_m+\tau)$和$\tilde{\Pi}_s(t_0,t)=[t_0,t]\backslash\tilde{\Pi}_a(t_0,t)$分别为DoS攻击区间和正常通信区间. 根据式(20), 对于$t\in[\tilde{t}_m+\tilde{\tau}_m+\tau,\tilde{t}_{m+1})$, 易得

$$V(t)\leqslant\mathrm{e}^{-\alpha_1(t-\tilde{t}_m-\tilde{\tau}_m-\tau)}V(\tilde{t}_m+\tilde{\tau}_m+\tau)\leqslant$$

$$\mathrm{e}^{-\alpha_1(t-\tilde{t}_m-\tilde{\tau}_m-\tau)}\mathrm{e}^{\alpha_2(\tilde{\tau}_m+\tau)}V(\tilde{t}_m)\leqslant$$
$$\cdots\leqslant$$
$$\mathrm{e}^{-\alpha_1\left|\tilde{\Pi}_s(t_0,t)\right|+\alpha_2\left|\tilde{\Pi}_a(t_0,t)\right|}V(t_0). \tag{21}$$

当$t\in[\tilde{t}_{m+1},\tilde{t}_{m+1}+\tilde{\tau}_{m+1}+\tau)$时, 通过同样的方法可以得到

$$V(t)\leqslant\mathrm{e}^{\alpha_2(t-\tilde{t}_{m+1})}V(\tilde{t}_m)\leqslant$$
$$\mathrm{e}^{\alpha_2(t-\tilde{t}_{m+1})-\alpha_1(\tilde{t}_{m+1}-\tilde{t}_m-\tilde{\tau}_m-\tau)}\cdot$$
$$V(\tilde{t}_m+\tilde{\tau}_m+\tau)\leqslant$$
$$\cdots\leqslant$$
$$\mathrm{e}^{-\alpha_1\left|\tilde{\Pi}_s(t_0,t)\right|+\alpha_2\left|\tilde{\Pi}_a(t_0,t)\right|}V(t_0). \tag{22}$$

在假设1和假设2下, 进一步可以推出

$$V(t)\leqslant\mathrm{e}^{-\alpha_1\left|\tilde{\Pi}_s(t_0,t)\right|+\alpha_2\left|\tilde{\Pi}_a(t_0,t)\right|}V(t_0)=$$
$$\mathrm{e}^{-\alpha_1(t-t_0)}\mathrm{e}^{(\alpha_1+\alpha_2)\left|\tilde{\Pi}_a(t_0,t)\right|}V(t_0)\leqslant$$
$$\mathrm{e}^{-\alpha_1(t-t_0)}\mathrm{e}^{(\alpha_1+\alpha_2)(\Pi_0+\frac{t-t_0}{T}+(1+n_0+\frac{t-t_0}{\tau_D})\tau)}\cdot$$
$$V(t_0)\leqslant\mathrm{e}^{(\alpha_1+\alpha_2)(\Pi_0+n_0\tau)}\cdot$$
$$\mathrm{e}^{-\left[\alpha_1-(\alpha_1+\alpha_2)\left(\frac{1}{T}+\frac{\tau}{\tau_D}\right)\right](t-t_0)}V(t_0). \tag{23}$$

令$\tilde{\Pi}_0=\Pi_0+n_0\tau$, 根据式(16)可得

$$\beta\triangleq\alpha_1-(\alpha_1+\alpha_2)\left(1/T+\tau/\tau_D\right)>0,$$

则式(23)可以重写为

$$V(t)\leqslant\mathrm{e}^{(\alpha_1+\alpha_2)\tilde{\Pi}_0}\mathrm{e}^{-\beta(t-t_0)}V(t_0). \tag{24}$$

然后, 有

$$V(t)\leqslant\mathrm{e}^{(\alpha_1+\alpha_2)\tilde{\Pi}_0}\mathrm{e}^{-\beta t}V(0). \tag{25}$$

这就意味着 $\lim\limits_{t\to\infty}V(t)=0$ 和 $\lim\limits_{t\to\infty}\varepsilon(t)=0$, $\lim\limits_{t\to\infty}\mathrm{e}(t)=0$. 从而有$\lim\limits_{t\to\infty}\left\|x_i(t)-\sum\limits_{j=1}^{N}x_j(t)\right\|=0$成立. 因此, 闭环系统(12)能够实现指数稳定.　　证毕.

注 4　对于不等式(14)–(15)解的存在性证明, 可具体参考文献[20]. 式(14)中通信拓扑已知且对于给定的$\mu_1>0$总有一个对应解P, 其数值解可通过MATLAB 线性矩阵不等式工具箱求得. 式(15)可写作$P(A-\frac{1}{2}\mu_2 I)+(A-\frac{1}{2}\mu_2 I)^{\mathrm{T}}P<0$为李雅普诺夫不等式, 一定存在解$P>0$使得式(15)成立.

4　数值仿真

在本节中, 给出了一个仿真例子来验证所提控制协议的有效性. 考虑一组含有4个智能体的同构多智能体系统. 智能体$i(i=1,2,3,4)$的动力学如下:

$$A=\begin{bmatrix}-0.38\,0.72\\-0.68\,0.42\end{bmatrix},\ B=\begin{bmatrix}0.5\\1\end{bmatrix}.$$

在本文中, 假设不同类型的传感器组有不同的采样周期, 即多率采样. 每一个智能体有两个状态分量, 并且状态分量x_{i1}和$x_{i2}(i=1,2,3,4)$的采样周期分别为0.05 s和0.09 s. 智能体之间的通信拓扑如图3所示. 在本例中, 智能体仅使用采样数据用于更新控制器和智能体间的通信. 值得注意的是, 当DoS攻击发生时, 采样数据不可用.

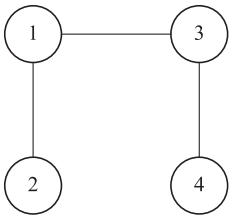

图 3　智能体之间的通信拓扑

Fig. 3　The communication topology among agents

根据定理1, 可以计算得到控制器增益矩阵$K=[0.4151\ \ 1.0671]$. 然后对于给定的初始状态$x_1(0)=[2\ \ 1]^{\mathrm{T}}$, $x_2(0)=[-3\ \ 2]^{\mathrm{T}}$, $x_3(0)=[5\ \ 0.5]^{\mathrm{T}}$和$x_4(0)=[-1\ \ -3]^{\mathrm{T}}$, 图5和图6分别给出了在本文所提方法和文献[21]中方法下, 智能体的状态轨迹演化过程. 其中, DoS攻击的开始时刻和持续时间均有随机函数随机生成, DoS攻击时序在图4给出.

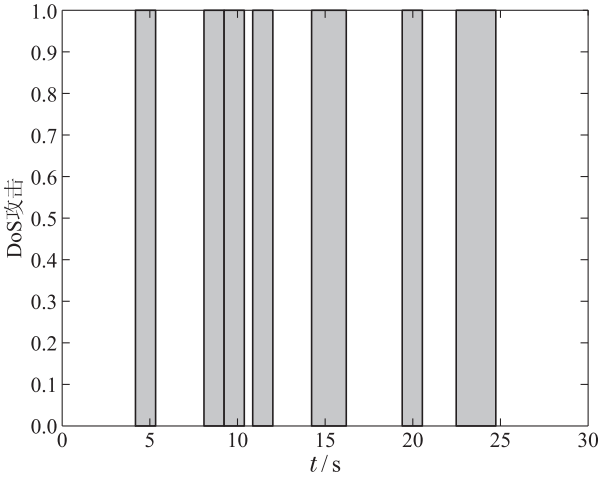

图 4　随机生成的DoS攻击时序

Fig. 4　Randomly generated DoS attack time sequence

从图5中可以看出, 在多率采样下, 第1次和第2次DoS攻击之间智能体的两个状态分量受其影响有小范围的波动, 但之后的几次DoS攻击并没有对多智能体系统的一致性造成破坏, 并且在大概15 s达到了状态一致. 图6给出了使用文献[21]中控制方法得到的受DoS攻击影响的多智能体系统(1)各智能体状态分量的响应. 从图6中可以看出, 在单率采样机制下, 所有智能体的状态在30 s左右达到一致性. 由此得出, 在多率采样机制下受到DoS攻击影响的多智能体系统一致性收敛速率更快, 效果更好.

在DoS攻击下, 采用多率采样策略与单率采样策略的一致性误差性能的对比结果在图7中给出, 其中一致性性能指标$E_q(t)=\sqrt{\sum\limits_{i=1}^{N}\omega_i^{\mathrm{T}}(t)\omega_i(t)}\ (t>0)$,

$\omega_i(t)=\sum\limits_{j=1}^{N}a_{ij}(x_j(t)-x_i(t))$. 由于多率采样策略的实时性, 控制器的更新次数明显多于单率采样, 故展现了更优异的一致性性能.

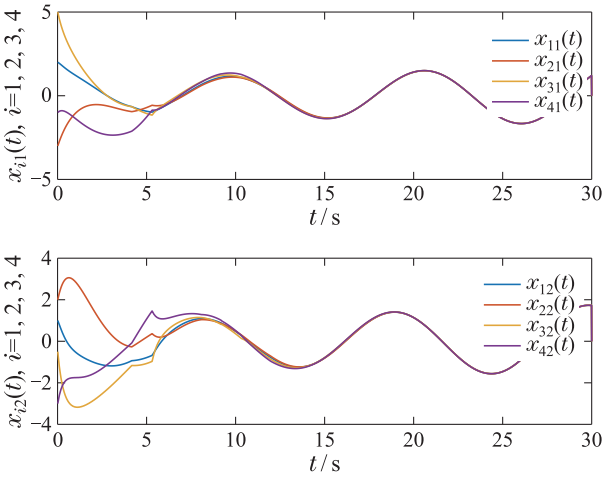

图 5 使用本文所提方法得到的多率采样下多智能体系统(1)在DoS攻击下的状态分量$x_{i1}(t), x_{i2}(t)(i=1,2,3,4)$的响应

Fig. 5 The response of state variable $x_{i1}(t)$,$x_{i2}(t)(i=1,2,3,4)$ of MAS(1) with multi-rate sampling under DoS attacks using the proposed method

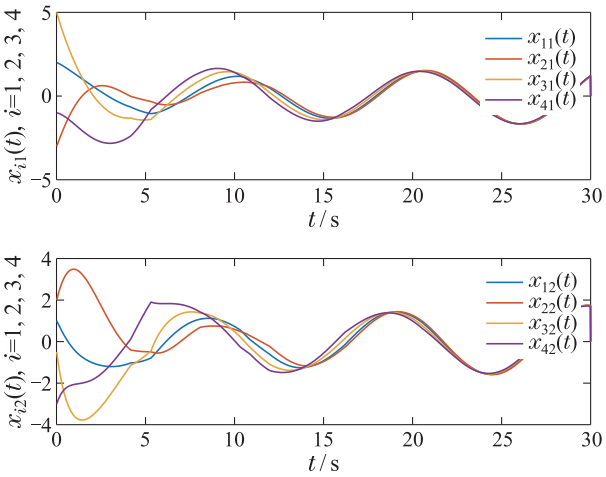

图 6 使用文献[21]控制方法得到多智能体系统(1)在DoS攻击下的状态分量$x_{i1}(t), x_{i2}(t)(i=1,2,3,4)$的响应

Fig. 6 The response of state variable $x_{i1}(t)$, $x_{i2}(t)(i=1,2,3,4)$ of MAS(1) under DoS attacks using the method in [21]

5 结论

本文对在DoS攻击下, 带有多率采样的线性多智能体系统的安全一致性控制问题进行了研究. 通过对攻击持续时间和攻击频率的限制得到了实现安全一致性的充分条件. 仿真和实验结果表明, 所设计的安全控制器可以保证带有多率采样的多智能体系统实现安全一致性, 并与单率采样进行了性能对比. 未来我们将研究更一般的网络攻击下带有多率采样的多智能体系统的安全协同问题.

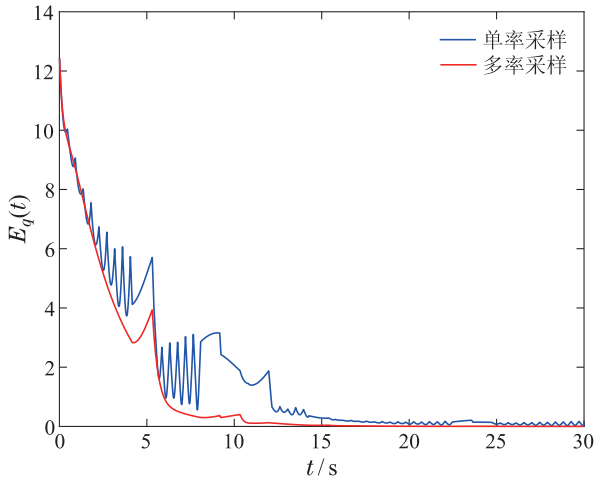

图 7 多智能体系统在DoS攻击下的单率采样与多率采样性能对比

Fig. 7 Single-rate sampling and multi-rate sampling performance comparison of multi-agent systems under DoS attacks

参考文献:

[1] QIN J, MA Q, SHI Y, et. al. Recent advances in consensus of multi-agent systems: A brief survey. *IEEE Transactions on Industrial Electronics*, 2017, 64(6): 4972 – 4983.

[2] XIE K, CHEN C, F. L. LEWIS, et al. Adaptive compensation for nonlinear time-varying multiagent systems with actuator failures and unknown control directions. *IEEE Transactions on Cybernetics*, 2019, 49(5): 1780 – 1790.

[3] PENG C, YUE D, FEI M R. A higher energy-efficient sampling scheme for networked control systems over IEEE 802.15.4 wireless networks. *IEEE Transactions on Industrial Informatics*, 2016, 12(5): 1766 – 1774.

[4] TIAN E, YUE D. Decentralized control of network-based interconnected systems: A state-dependent triggering method. *International Journal of Robust and Nonlinear Control*, 2015, 25(8): 1126 – 1144.

[5] GU Z, YUE D, TIAN E. On designing of an adaptive event-triggered communication scheme for nonlinear networked interconnected control systems. *Information Sciences*, 2017, 422: 257 – 270.

[6] ZHAO X, ZONG Q, TIAN B, et al. Integrated fault estimation and fault-tolerant tracking control for Lipschitz nonlinear multiagent systems. *IEEE Transactions on Cybernetics*, 2020, 50(2): 678 – 688.

[7] ZHANG W, TANG Y, HUANG T, et al. Sampled-data consensus of linear multi-agent systems with packet losses. *IEEE Transactions on Neural Networks and Learning Systems*, 2017, 28(11): 2516 – 2527.

[8] LIU W, HUANG J. Leader-following consensus for linear multiagent systems via asynchronous sampled-data control. *IEEE Transactions on Automatic Control*, 2020, 65(7): 3215 – 3222.

[9] LI B, JIA X C, CHI X, et al. Consensus for second-order multi-agent systems under two types of sampling mechanisms: A time-varying gain observer method. *IEEE Transactions on Cybernetics*, DOI: 10.1109/TCYB.2021.3052792.

[10] MA Weiwei, JIA Xinchun, ZHANG Dawei. Observer-based networked H_∞ control for dualrate sampling systems. *Acta Automatica Sinica*, 2015, 41(10): 1788 – 1797.
(马伟伟, 贾新春, 张大伟. 双率采样系统的基于观测器的网络化H_∞控制. 自动化学报, 2015, 41(10): 1788 – 1797.)

[11] MA W, JIA X C, ZHANG D. Networked continuous-time filtering for quadratically inner-bounded time-delay systems with multi-rate sampling. *Journal of the Franklin Institute*, 2017, 354(17): 7946 – 7967.

[12] CHI X, JIA X C, CHENG F. Networked H_∞ filtering for takagi-Sugeno fuzzy systems under multi-output multi-rate sampling. *Journal of the Franklin Institute*, 2019, 356(6): 3661 – 3691.

[13] JIA X C, GAO S, YOU X, et al. Output consensus of heterogeneous multi-agent systems with a multi-sensor multi-rate sampling mechanism. *Journal of the Franklin Institute*, 2020, 357(17): 12640 – 12669.

[14] C D PERSIS, P TESI. Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, 2015, 60(11): 2930 – 2944.

[15] LI Li, WANG Xijuan. Mean square consensus for leader-following multi-agent systems under denial-of- service attacks. *Control and Decision*, 2019, 34(11): 2317 – 2322.
(李丽, 王夕娟. 拒绝服务攻击下领导跟随多智能体系统的均方一致性研究. 控制与决策, 2019, 34(11): 2317 – 2322.)

[16] CHENG Z, YUE D, HU S, et al. Distributed event-triggered consensus of multi-agent systems under periodic DoS jamming attacks. *Neurocomputing*, 2020, 400: 458 – 466.

[17] XU Y, FANG M, SHI P, et al. Event-based secure consensus of multi-agent systems against DoS attacks. *IEEE Transactions on Cybernetics*, 2020, 50(8): 3468 – 3476.

[18] YANG Y, LI YF, YUE D. Event-trigger-based consensus secure control of linear multi-agent systems under DoS attacks over multiple transmission channels. *Science China Information Sciences*, 2020, 63(5): 150208:1 – 150208:14.

[19] TANG Y, ZHANG D, SHI P, et al. Event-based formation control for nonlinear multi-agent systems under DoS attacks. *IEEE Transactions on Automatic Control*, 2020, 66(1): 452 – 459.

[20] WU C, PAN W, SUN G, et al. Learning tracking control for cyber-physical systems. *IEEE Internet of Things Journal*, 2021, 8(11): 9151 – 9163.

[21] LI J Y, FANG F, LIU Y J, et al. Sampled-data-based consensus of distributed multi-agent systems under DoS attacks. *The IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*. Victoria, BC, Canada: IEEE, 2021: 647 – 652.

作者简介:

王　悦　硕士研究生, 研究方向为网络化控制系统、多智能体系统协同控制等, E-mail: wangyue5108@163.com;

贾新春　教授, 博士生导师, 主要研究方向为网络化控制系统、智能控制、无线传感网络等, E-mail: xchjia@sxu.edu.cn;

游　秀　副教授, 硕士生导师, 主要研究方向为多智能体协同控制、机器人控制、复杂非线性控制等, E-mail: xchjia@sxu.edu.cn;

吕　腾　硕士研究生, 研究方向为多智能体协同控制、事件触发控制等, E-mail: 2551495081@qq.com.