具有切换拓扑的多智能体系统协同控制的差分隐私保护

孙玉娇, 杨洪勇†, 于美妍

(鲁东大学 信息与电气工程学院, 山东 烟台 264025)

摘要: 网络信息技术的不断发展与普及使得各类数据的发布采集变得方便与便捷, 但数据的直接发布势必会造成个网络信息的泄露和敏感信息的失密, 因此敏感信息的保护成为了各行各业关注的问题. 本文研究了基于固定拓扑和切换拓扑的多智能体系统协同控制的差分隐私保护问题, 将差分隐私算法与传统平均一致性算法结合, 提出了具有隐私保护的协同控制算法, 分析了隐私保护算法对分布式协同控制闭环系统稳定性的影响. 基于所提算法, 应用矩阵论和概率统计对隐私保护协同控制算法的收敛性和隐私性进行理论分析, 该算法可以保护智能个体的数据隐私, 同时可以使得系统运动实现均方一致. 在系统拓扑结构动态变化的情况下, 本文对该算法的收敛性和隐私性进行理论分析, 讨论了切换拓扑对隐私保护的影响. 最后的仿真示例验证了理论结果的正确性.

关键词: 多智能体; 敏感信息; 差分隐私; 切换拓扑

引用格式: 孙玉娇, 杨洪勇, 于美妍. 具有切换拓扑的多智能体系统协同控制的差分隐私保护. 控制理论与应用, 2022, 39(7): 1345 – 1352

DOI: 10.7641/CTA.2021.10861

Differential privacy protection for cooperative control of multi-agent systems with switching topologies

SUN Yu-jiao, YANG Hong-yong†, YU Mei-yan

(School of Information and Electrical Engineering, Ludong University, Yantai Shandong 264025, China)

Abstract: With the continuous development and popularization of network information technology, the release and collection of all kinds of data become more and more convenient. However, the direct release of data will inevitably lead to the leakage of network information and the loss of sensitive information, so the protection of sensitive information has become a concern of all walks of life. In this paper, the differential privacy problem of cooperative control for first-order multi-agent systems based on fixed topology and switched topology is studied. A cooperative control algorithm with privacy is proposed by combining the differential privacy algorithm and the average consistency algorithm, and the influence of privacy protection algorithm on the stability of distributed cooperative control closed-loop system is analyzed. Based on the proposed algorithm, the convergence and the privacy of privacy protection cooperative control algorithm are theoretically analyzed by using matrix theory and probability statistics. The algorithm can protect the data privacy of intelligent individuals and make the system motion achieve mean square consistency. In the case of dynamic system topologies, the convergence and privacy of the algorithm is analyzed, and the impact of switching topologies on privacy protection is discussed. Finally, numerical simulations are shown to verify the correctness of the results.

Key words: multi-agent systems; sensitive information; differential privacy; switching topologies

Citation: SUN Yujiao, YANG Hongyong, YU Meiyan. Differential privacy protection for cooperative control of multi-agent systems with switching topologies. *Control Theory & Applications*, 2022, 39(7): 1345 – 1352

1 引言

在大数据的时代, 许多信息化平台通过用户数据可以为用户提供越来越方便的服务, 如: 定位服务、网上购物和健康服务等, 提高了服务质量和精度. 然而, 由于用户在享受便利服务的同时需要向平台提供自己的隐私信息, 如: 位置信息、兴趣爱好和身体状况等, 使得用户的信息被不可信任的第三方获取, 导致用户的隐私数据遭到严重的侵害. 因此, 隐私保护问题成为许多领域的研究者共同关注的问题.

近年来, 隐私保护被涉及到越来越多的问题当中,

收稿日期: 2021−09−13; 录用日期: 2021−11−11.

†通信作者. E-mail: hyyang@yeah.net; Tel.: +86 535-6681285.

本文责任编委: 孙长银.

国家自然科学基金项目(61673200)资助.

Supported by the National Natural Science Foundation of China (61673200).

如数据聚合问题. 文献[1]研究了自组织网络中的隐私保护数据聚合问题, 提出了具有隐私保护的基于一致性的数据聚合算法, 该算法在保护敏感数据隐私的同时保证了精确的聚合. 为了缓解数据收集和隐私保护的紧张, 差分隐私算法被认为是一个有效的解决方案. 差分隐私由Cynthia Dwork[2]提出, 差分隐私的定义要求协议或者机制保证一定范围内相邻的数据集通过该协议或机制输出在某一集合的概率的相差程度很小. 随着差分隐私的发展, 差分隐私已经被应用到许多不同的领域中, 如: 机器学习、多智能体一致性等等. 在考虑到隐私的情况下, 传统平均一致性算法中的智能体状态不可用, 使得传统平均一致性算法失效. 为了解决多智能体系统差分隐私平均一致性问题, 许多控制学者致力于设计出控制协议或机制使其不仅满足平均一致性, 而且满足差分隐私的定义, 以确保攻击者无法通过窃取通道信息获得智能体真实的位置信息. 文献[3]研究了差分隐私平均一致性问题, 提出了隐私算法, 保证了智能体状态的隐私性和平均一致性. 但这种算法不能让状态收敛到精确平均值, 只是平均值附近的一个随机值. 因此文献[4]研究了具有隐私保护的平均一致性问题, 提出了新的隐私保护平均一致性算法, 保证初始状态的隐私性和初始值精确平均值的渐近一致性. 文献[5]研究了考虑隐私保护的多智能体平均一致性问题, 提出了差分隐私一致性算法, 保证了智能体状态收敛到初始状态平均值的无偏估计, 并保护了智能体状态的隐私. 除此之外, 差分隐私被逐渐的拓展到越来越多不同多智能体系统中, 如事件触发系统、分布式优化系统等等. 文献[6] 研究了基于事件触发机制的差分隐私平均一致性问题, 提出了分布式事件触发机制差分隐私算法, 最终不仅保证了智能体初始状态隐私性, 而且可以提高整个系统的执行效率. 文献[7]研究了多智能体差分隐私分布式优化问题, 提出了基于拉格朗日的差分隐私分布式算法, 该算法不仅保证了智能体状态的隐私性, 而且系统具有更快的收敛速度. 文献[8]研究了轨迹隐私保护问题, 提出了基于差分隐私的轨迹保护算法, 该算法不仅保护了真实轨迹数据, 而且获得最后轨迹位置提高了数据发布的可用性. 文献[9]研究了差分隐私下多重一致性约束的最优发布问题, 提出了差分隐私一致性并行发布算法, 该算法不仅保证了数据的最优一致性发布, 而且提高了计算效率. 文献[10]研究了具有差分隐私保护的多智能体系统最大一致性问题, 提出了差分隐私最大一致性算法, 最终保证初始状态隐私性和初始状态最大值的渐进一致性.

随着智能机器人、传感器等设备的发展, 以及更复杂的实际应用的需求, 固定拓扑下的系统很难满足自动控制研究的现状. 在实际情况中, 固定拓扑系统可能会发生因通信能力、传感范围等限制因素导致的故障, 使得系统的通讯网络变得不连通, 因此研究切换拓扑对系统的影响具有很大的实际意义. 由于切换拓扑中拉普拉斯矩阵及其特征值也会随之发生变化, 使得理论分析过程变得相对复杂. 目前与切换拓扑的多智能体系统的相关研究已有不少. 文献[11]研究了非线性多智能体系统在切换拓扑下的基于事件触发的一致性控制问题, 提出了分布式事件触发一致性算法, 该算法得到了多智能体达到一致有界的充分条件, 并且降低了网络通信负载. 文献[12]研究了切换拓扑下离散和连续多智能体系统的一致性问题, 提出了一致性控制协议, 最终得到了智能体达到一致的充分条件. 文献[13]研究了时变拓扑下二阶多智能体系统有限时间一致性, 提出了有限时间一致性控制算法, 得到了多智能体在切换拓扑下达到有限时间一致的条件. 文献[14]研究了具有联合连通的时延的二阶多智能体系统一致性问题, 提出了时延控制算法, 得到了系统达到平均一致性的充分条件. 文献[15]研究了有向动态拓扑多智能体系统一致性控制问题, 提出了一致性控制算法, 得到了智能体达到指数一致的条件. 文献[16]研究了二阶动态拓扑系统跟踪虚拟领导者的问题, 提出了跟踪控制协议, 得到了联合连通条件下智能体协调跟踪控制的条件. 文献[17]研究了具有联合连通拓扑结构的做智能体系统领导跟随一致性问题, 提出了自适应一致性控制算法, 得到了领导者和跟随者渐近一致的条件. 文献[18]研究了具有不确定拓扑得多智能体系统的包容控制问题, 提出了具有时变的包容控制算法, 得到了多智能体系统分布式包容控制的约束条件.

从以上文献的研究发现, 对于切换拓扑的相关研究考虑了联合连通拓扑的情况, 联合连通拓扑是拓扑在某个时间段内进行若干次切换, 且不需要切换后的拓扑时刻连通, 这对降低通信成本、排除一定程度的通信链路故障具有很好的效果. 然而据作者所知, 对具有联合连通拓扑的多智能体系统隐私保护问题的相关研究很少.

受到已有研究成果的启发, 本文拟对具有切换拓扑多智能体系统的一致性的隐私保护进行研究. 本文的创新点主要是:

1) 本文提出了具有隐私保护的多智能体均方一致性控制算法, 该算法成功结合了传统平均一致算法和差分隐私算法, 可以保护智能个体的数据隐私, 同时可以使得系统运动实现均方一致.

2) 当多智能体系统的连接拓扑是动态变化不连通的情况下, 本文研究了具有切换拓扑的多智能体系统协同控制的隐私保护问题, 对该算法的收敛性和隐私性进行理论分析, 并讨论了切换拓扑对隐私保护的影响.

2　问题描述

2.1　代数图论与概率理论

用无向图$G=\{V,E\}$描述n个智能体的通信拓扑图, $V=(v_1,v_2,\cdots,v_n)$表示节点集合, $E\subseteq V\times V$表示边集合. 记智能体i的邻域为$N_i=\{j|(j,i)\in E, \forall j\in V\}$. 图$G$对应的邻接矩阵为$A=[a_{ij}]$, 其中$a_{ij}$表示智能体$i$和智能体$j$之间的连接权重, 当且仅当智能体$i$与它邻域中的任一智能体之间有通信时, $a_{ij}>0$, 否则$a_{ij}=0$. Laplacian矩阵为$L=D-A$, 其中度矩阵D是一个对角矩阵, 表示为$D=\mathrm{diag}\{d_1,d_2,\cdots,d_n\}$, $d_i=\sum\limits_{j\neq i}a_{ij}$. 在一个无向图$G$中, 若从顶点$i$到顶点$j$有路径相连(当然从$j$到$i$也一定有路径), 则称$i$和$j$是连通的. 如果图中任意两点都是连通的, 那么图被称作连通图.

假设x表示一个服从均值为0, 方差为$2b^2$的拉普拉斯分布的随机变量, 记作$x\sim\mathrm{Lap}(\mu,b)$, 它的概率密度函数表示为$f=\dfrac{1}{2b}\mathrm{e}^{-\frac{|x|}{b}}$, 其中$b>0$.

2.2　相关引理和定义

引理 1[12]　如果一组无向图的并集G_{1-n}是连通, 那么称这组图是联合连通的, 矩阵的积

$$\mathrm{e}^{C(t_m)(t_m-t_{m-1})}\cdots\mathrm{e}^{C(t_2)(t_2-t_1)}\mathrm{e}^{C(t_1)(t_1-t_0)}$$

为SIA (不可约非周期矩阵), 其中矩阵$C(t_i)$是无向图G_{t_i}对应的矩阵.

引理 2[12]　令$S_1,S_2,\cdots,S_k$是一个有限的SIA矩阵序列, 对于每一个长度为正的序列$S_{i_1},S_{i_2},\cdots,S_{i_j}$, 矩阵的积$S_{i_j}S_{i_{j-1}}\cdots S_{i_1}$为SIA, 那么对于每一个无限序列$S_{i_1},S_{i_2},\cdots$, 存在一个向量$y$使得

$$\lim_{j\to\infty}S_{i_j}S_{i_{j-1}}\cdots S_{i_1}=1y^{\mathrm{T}}$$

成立.

引理 3[12]　设正整数$m>2$, 如果$P_1,P_2,\cdots,P_m$是具有正对角元素的非负$n\times n$矩阵, 那么

$$P_1P_2\cdots P_m\geqslant\gamma(P_1+P_2+\cdots P_m),\tag{1}$$

其中$\gamma>0$可以由矩阵P_i指定.

定义 1　对于任意智能体i,j, 多智能体系统能够实现均方一致性, 如果以下等式成立:

$$\lim_{t\to\infty}\mathrm{E}[(x_i(t)-x_j(t))^2]=0,\tag{2}$$

其中x_i表示智能体状态.

定义 2　对于两组数据$x\in\mathbb{R}^n,x'\in\mathbb{R}^n$, 隐私保护的敏感度定义如下:

$$\Delta f=\max_{x,x'\in D}\|x'-x\|_d,\tag{3}$$

其中$d=1$.

定义 3　向量$x\in\mathbb{R}^n,x'\in\mathbb{R}^n$被称为是$\Delta f$–邻接的, 如果以下不等式成立:

$$\|x'-x\|_1\leqslant\Delta f,\tag{4}$$

其中Δf表示敏感度.

定义 4　已知一对Δf邻接的状态向量x,x', 多智能体系统满足ε–差分隐私, 如果以下不等式成立:

$$\Pr[M(D)\in O]\leqslant\mathrm{e}^{\varepsilon}\Pr[M(D')\in O],\tag{5}$$

其中: $\Pr[\cdot]$表示算法执行后的观测序列构成的集合的概率, $M(\cdot)$表示算法的执行, O表示观测序列, $\varepsilon>0$表示隐私保护预算.

3　具有固定拓扑的多智能体系统的隐私保护

3.1　均方一致性

考虑n个智能体的协同运动问题, 假设第i个智能体的运动方程为

$$\dot{x_i}=u_i,\tag{6}$$

其中: $x_i\in\mathbb{R}$表示智能体i的位置, $u_i\in\mathbb{R}$表示智能体i的控制输入.

假设$\tilde{x}_i$是加密状态, 则隐私保护算法的表达式表示为

$$\tilde{x}_i=x_i+w_i,\tag{7}$$

其中w_i是服从均值为0, 方差为$2b^2$拉普拉斯分布的噪声, 记作$x\sim\mathrm{Lap}(\mu,b)$.

假设 1　对任意智能体$i,j\in\{1,2,\cdots,n\}, i\neq j$, x_i, w_i相互独立, w_i,w_j相互独立.

注 1　隐私算法保证了智能体i与它的邻域中的任一智能体通信的状态不是真实状态, 而是加密状态.

通过以上的分析，该系统的动态方程可以表示为

$$\begin{cases}\dot{x}_i(t)=u_i,\\ u_i=\dfrac{1}{d_i}\sum\limits_{j\in N_i}a_{ij}(x_j(t)-x_j(t)),\end{cases}\tag{8}$$

其中: 对于连通网络有$\sum\limits_{j\in N_i}\dfrac{a_{ij}}{d_i}=1, d_i=\sum\limits_{j\in N_i}a_{ij}>0$.

设$c_{ij}=\dfrac{a_{ij}}{d_i}$, 系统的隐私保护一致性控制算法表示为

$$u_i=\sum_{j\in N_i}c_{ij}(x_j(t)-x_j(t)),\ i=1,2,\cdots,n.\tag{9}$$

引理 4　若非负矩阵$C=[c_{ij}]\in\mathbb{R}^{n\times n}$是一个随机矩阵, 则矩阵有以下性质:

1) 特征值满足$\lambda_1=1,|\lambda_i|<1,i=2,3,\cdots,n$.

2) $C1=1$, 其中$1=(1\ \ 1\ \ \cdots\ \ 1)^{\mathrm{T}}$是特征值1对应的特征向量.

注 2　如果在控制协议中选取$c_{ij}\geqslant0$且满足$\sum\limits_{j\in N_i}c_{ij}=1$也能够有引理4的结论.

将系统写成矩阵形式

$$\dot{x}(t) = -L(x(t) + w(t)), \tag{10}$$

其中: 矩阵$L = E - C$, E表示单位矩阵, $w = (w_1\ w_2\ \cdots\ w_n)^{\mathrm{T}}$表示隐私保护噪声向量.

注 3 通过构造的隐私一致性算法(9)可以看到, 网络传输的信息是经过加密的隐私数据, 在网络传递时隐藏了智能体的真实信息, 即使攻击者窃取通道传输信息, 也不会获得智能体真实数据信息, 这样就保护了智能体的隐私. 这是本文算法与传统平均一致性算法的区别. 协同控制采用隐私保护的意义在于保护智能体的敏感数据同时使得多智能体系统实现均方一致.

注 4 如果不给网络传输信息加密, 那么攻击者获取智能体真实数据后, 可能会对多智能体系统的运行造成负面影响. 例如, 当智能体i的初始状态信息泄露后, 攻击者使用相同的初始状态进行冒充, 并且切掉智能体i与邻居智能体的连接, 最终使得多智能体系统的运行受到破坏.

定理 1 考虑一个具有n个智能体的系统, 它的运动方程为式(6), 智能体的加密算法为式(7), 在隐私保护一致性控制算法(9)的作用下, 智能体位置会渐近收敛到均方一致, 并且智能体位置的隐私得到了保护.

证 由无向图的性质可知, 矩阵Laplacian有一个0特征值, 其余特征值均大于0. 假设$\lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_n, \forall i, \lambda_i \geqslant 0, \lambda_1 = 0$, λ_1对应的特征向量$v_1 = (1\ \ 1\ \cdots\ 1)^{\mathrm{T}}$. 已知线性定常系统状态方程(8)的零解为

$$x(t) = \mathrm{e}^{-Lt}x(0) + \int_0^t \mathrm{e}^{-L(t-\tau)}(-L)w(\tau)\mathrm{d}\tau. \tag{11}$$

分析方程(8)的零解. 由于矩阵L有一个特征值为0, 因此存在正交矩阵P使得矩阵L相似对角化, 即$P^{\mathrm{T}}LP = \Lambda = \mathrm{diag}\{0, \lambda_2, \cdots, \lambda_n\}$, 其中$\lambda_i$是矩阵$L$的$n-1$个不为0的特征值. 由于特征值0对应的特征向量为$(1\ \ 1\ \ \cdots\ \ 1)^{\mathrm{T}}$, 则正交矩阵$P = (p_1, p_2, \cdots, p_n)$的第1列表示为

$$p_1 = (\frac{1}{\sqrt{n}}\ \ \frac{1}{\sqrt{n}}\ \ \cdots\ \ \frac{1}{\sqrt{n}})^{\mathrm{T}},$$

P^{T}的第1行表示为

$$\bar{p}_1 = (\frac{1}{\sqrt{n}}\ \ \frac{1}{\sqrt{n}}\ \ \cdots\ \ \frac{1}{\sqrt{n}}),$$

因此式(11)的第1项表示为

$$y(t) = \mathrm{e}^{-Lt}x(0) = PQP^{\mathrm{T}}x(0), \tag{12}$$

其中$Q = \mathrm{diag}\{1, \mathrm{e}^{-\lambda_2 t}, \cdots, \mathrm{e}^{-\lambda_n t}\}$. 因此可以得到

$$\lim_{t\to\infty} y(t) = \frac{1}{n}\sum_{i=1}^{n} x_i(0). \tag{13}$$

由于$w(t)$服从期望为0的Laplace分布, 因此对式(11)两边求期望可得

$$\mathrm{E}[\lim_{t\to\infty} x(t)] = \frac{1}{n}\sum_{i=1}^{n} x_i(0). \tag{14}$$

根据定义1, 该分布式系统是渐近稳定的, 智能体的状态渐近收敛到均方一致, 收敛点为所有智能体初始值的平均值, 即$\dfrac{1}{n}\sum\limits_{i=1}^{n} x_i(0)$. 证毕.

3.2 隐私保护算法分析

为了保护任意智能体的位置状态的隐私, 给智能体真实位置加上一个服从拉普拉斯分布的噪声得到发送位置, 使得后续状态更新过程中不会再出现与真实状态相关的信息.

定理 2 给定一对Δf–邻接的状态向量x和x', 则隐私保护一致性控制算法(9)提供ε–隐私保护, 其中$\varepsilon > 0$.

证 用$x(t) = (x_1(t)\ \ x_2(t)\ \cdots\ \ x_n(t))^{\mathrm{T}}$表示智能体的真实状态, 用$\tilde{x}(t) = (\tilde{x}_1(t)\ \tilde{x}_2(t)\ \cdots\ \tilde{x}_n(t))^{\mathrm{T}}$表示网络系统从初始时刻开始的加密信息, 根据定义2可知差分隐私敏感度为

$$\Delta f = \max(\|x - x'\|_1) = \max(\sum_{i=1}^{n} |x - x'|). \tag{15}$$

假设Laplace噪声的参数设定为$b = \dfrac{\Delta f}{\varepsilon}$, 此时Laplace噪声变量的概率密度函数表示为

$$g(w_i) = \frac{\varepsilon}{2\Delta f}\mathrm{e}^{-\frac{\varepsilon|w_i|}{\Delta f}},$$

根据假设1, 噪声变量w_i, w_j相互独立, 因此添加到n个智能体的噪声变量的概率密度函数可以表示为

$$g(w) = \prod_{i=1}^{n} \frac{\varepsilon}{2\Delta f}\mathrm{e}^{-\frac{\varepsilon|w_i|}{\Delta f}}.$$

根据加密算法(7), 添加到每个智能体的噪声变量可以表示为$w_i = \tilde{x} - x_i$, 如果Δf–邻接的状态向量x_i'的加密状态向量也是$\tilde{x}$, 那么根据加密算法将添加到每个智能体的噪声变量表示为$w_i = \tilde{x}_i - x_i'$. 根据以上的分析, 添加到n个智能体的噪声变量的概率密度函数可以表示为

$$\prod_{i=1}^{n} \frac{\varepsilon}{2\Delta f}\mathrm{e}^{-\frac{\varepsilon|\tilde{x}-x_i|}{\Delta f}} \text{ 和 } \prod_{i=1}^{n} \frac{\varepsilon}{2\Delta f}\mathrm{e}^{-\frac{\varepsilon|\tilde{x}-x_i'|}{\Delta f}}.$$

假设添加到Δf–邻接的状态向量x, x'的噪声变量的概率密度函数用ρ_1, ρ_2表示, 那么可以得到以下不等式:

$$\frac{\rho_1}{\rho_2} = \frac{\prod\limits_{i=1}^{n} \frac{\varepsilon}{2\Delta f}\mathrm{e}^{-\frac{\varepsilon|\tilde{x}_i-x_i|}{\Delta f}}}{\prod\limits_{i=1}^{n} \frac{\varepsilon}{2\Delta f}\mathrm{e}^{-\frac{\varepsilon|\tilde{x}_i-x_i'|}{\Delta f}}} \leqslant \prod_{i=1}^{n} \mathrm{e}^{\frac{\varepsilon|x_i-x_i'|}{\Delta f}} \leqslant \mathrm{e}^{\varepsilon}. \tag{16}$$

对式(16)两边求积分后可以得到$\Pr[M(x) \in O] \leqslant \mathrm{e}^{\varepsilon}\Pr[M(x') \in O]$. 也就是说, 对于$\Delta f$邻接的状态

向量x, x', 使用隐私保护协同控制算法得到相同的观测向量$\tilde{x}$的概率是非常大的. 换句话说, 攻击者试图从观测序列中估计噪声进而推断出准确的真实状态的概率是非常小的. 这说明了隐私保护一致性控制算法保证了相似的输入有大致相同的输出, 使得攻击者无法从截取的观测信息中区分x, x', 因此智能体系统的真实状态向量x受到隐私保护.

下面分析隐私保护强度. 取$\varepsilon = \dfrac{\Delta f}{b}$, 在噪声方差一定的条件下, Δf越小, ε就越小, 隐私保护算法提供的隐私保护强度就越高, 这说明两个向量之间的差值越小, 噪声对真实数据的保护就越好.　　证毕.

4　具有切换拓扑的多智能体系统的隐私保护

4.1　均方一致性

假设有一个无限的时间序列$t_0, t_1, t_2, \cdots$, 从$t_0 = 0$开始在这个时间序列中存在有限个有界的时间间隔$[t_k, t_{k+1}),\ k = 0, 1, \cdots$ 满足$t_{k+1} - t_k \leqslant T_1,\ T_1 > 0$, 同时在每个时间间隔内存在有限个子时间间隔$[t_{k_{k,0}}, t_{k_{k,1}}), [t_{k_{k,1}}, t_{k_{k,2}}), \cdots, [t_{k_{k,s-1}}, t_{k_{k,s}})$满 足$t_{k_{k,0}} = t_k$, $t_{k_{k,s}} = t_{k+1}, t_{k_{k,s}} - t_{k_{k,s-1}} \geqslant T_2,\ 0 < T_2 < T_1$. 假设多智能体系统的拓扑图在子时间间隔里可能是不连通的, 即在子时间间隔$[t_{k_{k,0}}, t_{k_{k,1}})$中只有$n_1$个智能体之间是有连接的, 此时拓扑图记为$G_{k,1}$, 而在子时间间隔$[t_{k_{k,1}}, t_{k_{k,2}})$中只有$n_2$个智能体连接, 拓扑图记为$G_{k,2}$, 以此类推, 其中$n_1 < n,\ n_2 < n, \cdots, n_s < n$. 如果在时间间隔$[t_k, t_{k+1})$内多智能体系统的拓扑图的并集$G_{k,1-s}$是连通的, 那么称多智能体系统在时间间隔$[t_k, t_{k+1})$内是联合连通的.

定理 3　考虑具有n个智能体的系统, 智能体的运动方程为式(6), 智能体加密算法为式(7), 在算法(9)的作用下, 如果智能体系统在无穷时间序列$t_0, t_1, t_2, \cdots$的每个时间间隔$[t_k, t_{k+1})$都是联合连通的, 那么任意智能体的位置将会渐近收敛到均方一致, 并且任意智能体的真实状态受到保护.

证　假设在子时间间隔$[t_{k_{k,0}}, t_{k_{k,1}})$内有$n_1$个智能体连接, 那么该定常子系统的矩阵形式表示为

$$\dot{x}(t) = -L_{k,1}(x(t) + w(t)). \tag{17}$$

当$t = t_{k_{k,1}}$时, 该定常子系统的解表示为

$$x(t_{k_{k,1}}) = \mathrm{e}^{-L_{k,1}(t_{k_{k,0}})(t_{k_{k,1}} - t_{k_{k,0}})} x(t_{k_{k,0}}). \tag{18}$$

假设在子时间间隔$[t_{k_{k,1}}, t_{k_{k,2}})$内有$n_2$个智能体连接, 那么该定常子系统的矩阵形式表示为

$$\dot{x}(t) = -L_{k,2}(x(t) + w(t)). \tag{19}$$

当$t = t_{k_{k,2}}$时, 该定常子系统的解表示为

$$x(t_{k_{k,2}}) = \mathrm{e}^{-L_{k,2}(t_{k_{k,1}})(t_{k_{k,2}} - t_{k_{k,1}})} x(t_{k_{k,1}}). \tag{20}$$

以此类推, 迭代后得到时间间隔$[t_k, t_{k+1})$的子系统的解, 表示为

$$\begin{aligned} x(t_{k+1}) = {} & \exp(-L_{k,s}(t_{k_{k,s-1}})(t_{k_{k,s}} - t_{k_{k,s-1}}) - \\ & \cdots - L_{k,2}(t_{k_{k,1}})(t_{k_{k,2}} - t_{k_{k,1}}) - \\ & L_{k,1}(t_{k_{k,0}})(t_{k_{k,1}} - t_{k_{k,0}}))x(t_{k_{k,0}}). \end{aligned} \tag{21}$$

经过类似的分析, 通过迭代可以得到系统在无穷时间序列的解表示为

$$\begin{aligned} x(t) = {} & \exp(-L_{k,s}(t_{k_{k,s}})(t - t_{k_{k,s}}) - \\ & \cdots - L_{k,2}(t_{k_{k,1}})(t_{k_{k,2}} - t_{k_{k,1}}) - \\ & L_{k,1}(t_{k_{k,0}})(t_{k_{k,1}} - t_{k_{k,0}}))x(t_{k_{k,0}}), \end{aligned} \tag{22}$$

其中$k = 0, 1, 2, \cdots$.

已知时间间隔$[t_k, t_{k+1})$内系统的拓扑图的并集$G_{k,1-s}$是连通的, 根据引理1, 矩阵的积

$$\begin{aligned} & \exp(-L_{k,s}(t_{k_{k,s-1}})(t_{k_{k,s}} - t_{k_{k,s-1}}) - \cdots - \\ & L_{k,2}(t_{k_{k,1}})(t_{k_{k,2}} - t_{k_{k,1}}) - \\ & L_{k,1}(t_{k_{k,0}})(t_{k_{k,1}} - t_{k_{k,0}}))x(t_{k_{k,0}}) \end{aligned}$$

是SIA的, 根据引理3, 矩阵$\mathrm{e}^{-L_{k,s}(t_{k_{k,s-1}})(t_{k_{k,s}} - t_{k_{k,s-1}})}$是随机矩阵, 结合引理2可得

$$\begin{aligned} & \exp(-L_{k,s}(t_{k_{k,s}})(t - t_{k_{k,s}}) - \cdots - \\ & L_{k,2}(t_{k_{k,1}})(t_{k_{k,2}} - t_{k_{k,1}}) - \\ & L_{k,1}(t_{k_{k,0}})(t_{k_{k,1}} - t_{k_{k,0}}))x(t_{k_{k,0}}) \end{aligned}$$

是SIA的, 也就是存在向量使得以下等式成立:

$$\begin{aligned} & \lim_{t\to\infty} \exp(-L_{k,s}(t_{k_{k,s}})(t - t_{k_{k,s}}) - \cdots - \\ & L_{k,2}(t_{k_{k,1}})(t_{k_{k,2}} - t_{k_{k,1}}) - \\ & L_{k,1}(t_{k_{k,0}})(t_{k_{k,1}} - t_{k_{k,0}}))x(0) = \\ & \frac{1}{n}\sum_{i=1}^{n} x_i(0). \end{aligned} \tag{23}$$

由于$w(t)$服从期望为0的Laplace分布, 因此对系统的解两边求期望可得

$$\mathrm{E}[\lim_{t\to\infty} x(t)] = \frac{1}{n}\sum_{i=1}^{n} x_i(0). \tag{24}$$

这意味着多智能体系统在联合连通条件下能够渐近收敛到均方一致性, 且最终收敛值是智能体初始值的平均值.　　证毕.

4.2　隐私保护算法分析

定理 4　给定一对Δf–邻接的状态向量x, x', 隐私控制算法能够提供$\sum_i \varepsilon_i$–隐私保护, 其中$\varepsilon_i > 0$.

证　考虑子区间$[t_{k_{k,0}}, t_{k_{k,1}})$内的多智能体系统, 假设在该区间内有$n_1$个智能体连接, 这些智能体在该时间段内的位置向量表示为$x(t) = (x_{l_{1,1}}\ x_{l_{2,2}}\ \cdots\ x_{l_{n_1,1}})^{\mathrm{T}}$, 加密位置向量表示为$\tilde{x}(t) = (\tilde{x}_{l_{1,1}}\ \tilde{x}_{l_{2,1}}\ \cdots\ \tilde{x}_{l_{n_1,1}})^{\mathrm{T}}$, 根据敏感度定义可以得到

$$\Delta f = \max(\|x - x'\|_1) = \max(\sum_{i=1}^{n} |x - x'|). \tag{25}$$

已知敏感度来假设噪声参数$b = \dfrac{\Delta f}{\varepsilon_1}$, 根据前面类似的分析, 此时$n_1$个智能体噪声变量概率密度函数表示为

$$\prod_{i=l_{1,1}}^{l_{n_1,1}} \frac{\varepsilon_1}{2\Delta f} \mathrm{e}^{-\frac{\varepsilon_1|\tilde{x}-x_i|}{\Delta f}} \text{ 和 } \prod_{i=l_{1,1}}^{l_{n_1,1}} \frac{\varepsilon_1}{2\Delta f} \mathrm{e}^{-\frac{\varepsilon_1|\tilde{x}-x'_i|}{\Delta f}}.$$

假设分别用$\rho_{1,1}$和$\rho_{2,2}$表示, 那么可以得到

$$\frac{\rho_{1,1}}{\rho_{2,2}} = \frac{\prod\limits_{i=l_{1,1}}^{l_{n_1,1}} \dfrac{\varepsilon_1}{2\Delta f} \mathrm{e}^{-\frac{\varepsilon_1|\tilde{x}_i-x_i|}{\Delta f}}}{\prod\limits_{i=l_{1,1}}^{l_{n_1,1}} \dfrac{\varepsilon_1}{2\Delta f} \mathrm{e}^{-\frac{\varepsilon|\tilde{x}_i-x'_i|}{\Delta f}}} \leqslant \prod_{i=l_{1,1}}^{l_{n_1,1}} \mathrm{e}^{\frac{\varepsilon_1|x_i-x'_i|}{\Delta f}} \leqslant \mathrm{e}^{\varepsilon_1}. \tag{26}$$

对式(26)求积分可以得到$\Pr[M(x) \in O] \leqslant \mathrm{e}^{\varepsilon_1} \Pr[M(x') \in O]$, 也就是说在子区间$[t_{k_{k,s-1}}, t_{k_{k,s}})$内隐私保护一致性控制算法能够保证攻击者无法从观测序列区分x, x', 因此向量x受到保护.

同样的道理, 隐私保护算法在区间$[t_{k_{k,s-1}}, t_{k_{k,s}})$内提供$\varepsilon_s$–隐私保护. 综合以上的分析, 在具有切换拓扑的多智能体系统中, 隐私保护算法能够提供$\sum\limits_i \varepsilon_i$–隐私保护. 证毕.

5 仿真示例

5.1 具有固定拓扑的多智能体系统的隐私保护

为了验证本文算法的效果, 本文考虑由6个智能体组成的多智能体系统, 每个智能体的初始状态取值为$x(0) = [-6.5, 5.4, -9.6, 10.3, 6.9, 4.2]$, 假设多智能体系统的无向通信拓扑图如图1所示.

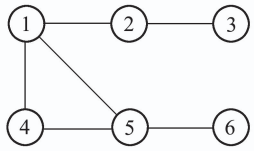


图 1 多智能体系统的通信拓扑图

Fig. 1 The communication topology of multi-agent systems

图2表示在隐保护私协同控制算法作用下所有智能体的位置状态, 从图中可以看出多智能体状态最终都渐近收敛到初始状态的平均值, 这说明了隐私保护协同控制算法不会影响多智能体系统的收敛性. 图3表示在传统平均一致性控制算法作用下和在隐私保护协同控制算法作用下所有智能体位置状态的误差, 从图中可以看出这两个状态之间一直存在一个很小的偏差, 产生这种偏差的原因是在隐私保护协同控制算法中的智能体真实状态被加密状态代替; 偏差很小的原因是隐私保护协同控制算法能够保证相似的输入有大致相同的输出, 这也说明了攻击者无法准确的区分智能体真实状态, 使得智能体的真实状态受到保护. 图4表示智能体的控制器随时间变化图, 从图中可以看出随着智能体的状态收敛到初始状态的平均值, 智能体的控制器状态逐渐趋于0.

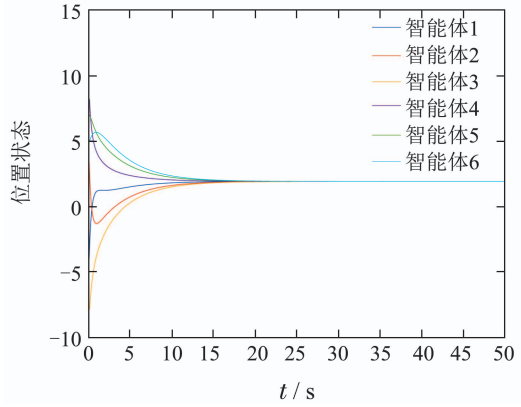


图 2 具有隐私保护的智能体位置状态

Fig. 2 The position states of agents with privacy protection

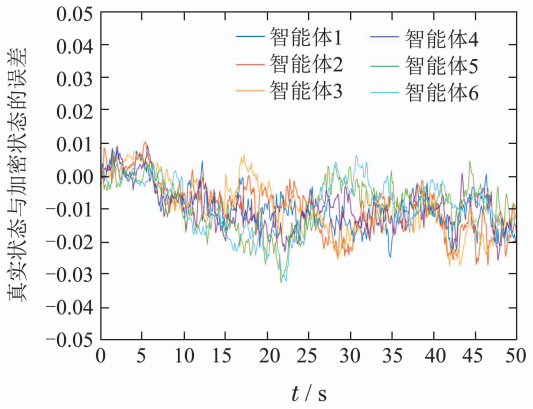


图 3 智能体真实状态与加密状态的误差

Fig. 3 The errors of agents between actual value and encrypted value

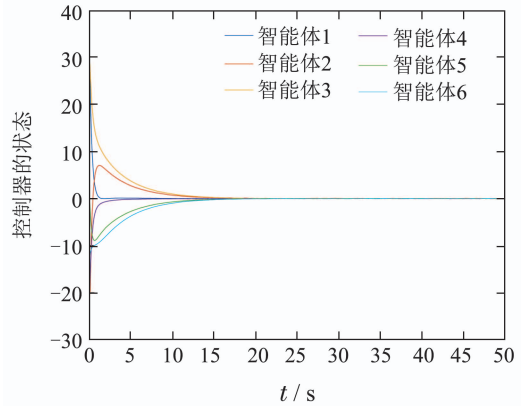


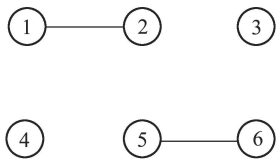
图 4 智能体的控制器状态

Fig. 4 The controller states of agents

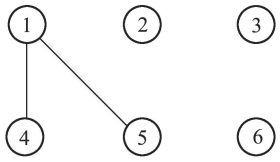
通过仿真可以发现, 本文的提出的差分隐私协同控制算法是在传统平均一致性算法的基础上提出的, 结合差分隐私算法后, 使得智能体状态逐渐收敛到均方意义下的平均一致性. 相比传统平均一致性算法, 本文算法能够保护智能体真实状态, 而传统平均一致性算法不能保护智能体状态.

5.2　具有切换拓扑的多智能体系统的隐私保护

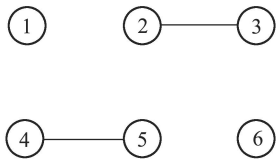
假设6个智能体在时间间隔$[t_{i-1}, t_i)$内按照图5所示拓扑图依次进行切换, 那么多智能体系统在隐私保护协同控制算法的作用下的仿真结果如下图所示.



(a) 通信拓扑图1



(b) 通信拓扑图2



(c) 通信拓扑图3

图 5　智能体切换通信拓扑图

Fig. 5　The switching communication topologies of multi-agent systems

图6表示在隐私保护协同控制算法作用下所有智能体位置状态, 从图中可以看出所有智能体的位置状态随着时间的变化最终都趋向于初始状态的平均值, 这说明了隐私保护协同控制算法不会影响多智能体系统的收敛性. 而且从图6可以看出智能体的状态曲线图是不光滑的, 产生不光滑曲线的原因是在时间间隔内有的智能体没有与别的智能体产生连接, 进而没有位置更新. 图7表示在传统平均一致性协同控制算法和本文提出的隐私保护协同控制算法作用下所有智能体状态的误差, 从图中可以看出所有智能体的真实状态与加密状态的误差一直在一个很小的范围内, 产生这种偏差的原因是在隐私保护协同控制算法中的智能体真实状态被加密状态代替; 偏差很小的原因是隐私保护协同控制算法能够保证相似的输入有大致相同的观测序列, 这保证了攻击者无法准确的区分智能体真实状态, 也就使得智能体的真实状态受到保护.

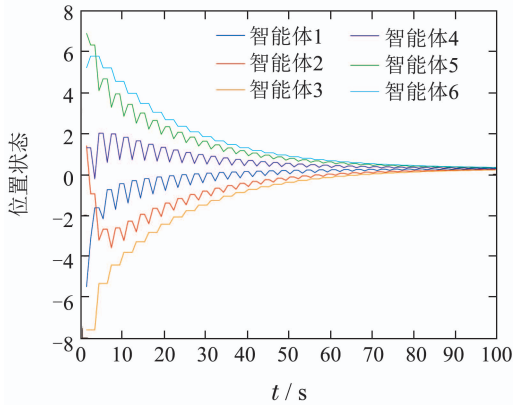


图 6　具有隐私保护的智能体位置状态

Fig. 6　The position states of agents with privacy protection

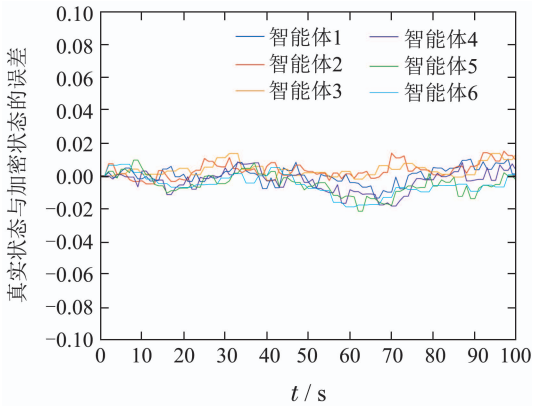


图 7　智能体真实状态与加密状态的误差

Fig. 7　The errors of agents between actual value and encrypted value

对比图3和图7可以看出, 隐私保护算法在固定拓扑和切换拓扑的情况下都可以保护个体数据隐私, 真实数据与加密数据之间都会有一个很小的偏差, 也就是切换拓扑不会影响个体数据的隐私保护. 但通过对比还可以发现, 切换拓扑对施加保护的系统的收敛性来说, 会使得系统收敛性分析更加复杂, 也会影响系统的收敛速度.

5.3　隐私泄露

在本节中, 将对隐私泄露后的系统进行仿真分析. 假设1号智能体的被攻击, 攻击者冒充1号智能体, 并切断1号智能体与邻居智能体的连接.

图8表示隐私泄露后智能体状态随着时间变化的曲线图, 从图中可以看出, 1号智能体表示隐私泄露的智能体, 该智能体状态保持不变, 2号和3号智能体状态最终都保持−2.1不变, 4号, 5号和6号智能体状态最终都保持7.1不变. 这说明了隐私泄露对系统造成无法收敛的影响, 使得系统的稳定性受到破坏.

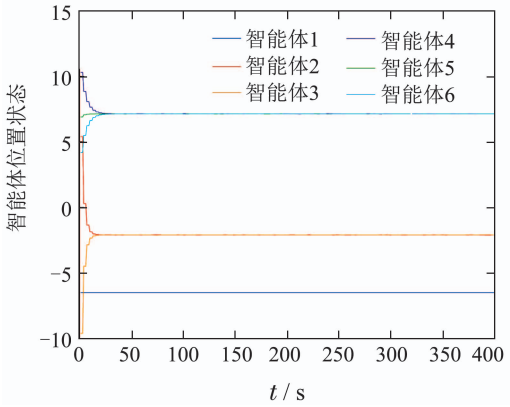


图 8 具有隐私泄露的智能体位置状态

Fig. 8 The position states of agents with privacy leak

图9表示隐私保护强度随着尺度参数变化的曲线图, 红色曲线表示在$\Delta f = 0.3$时, 隐私保护强度随着尺度参数的变化情况, 蓝色曲线表示在$\Delta f = 0.6$时, 隐私保护强度随着尺度参数的变化情况. 从图中可以看出, 在Δf一定时, 随着尺度参数b越来越大, ε会越来越小, 也就是隐私保护算法的隐私保护强度会越来越高, 算法对数据的保护性越好.

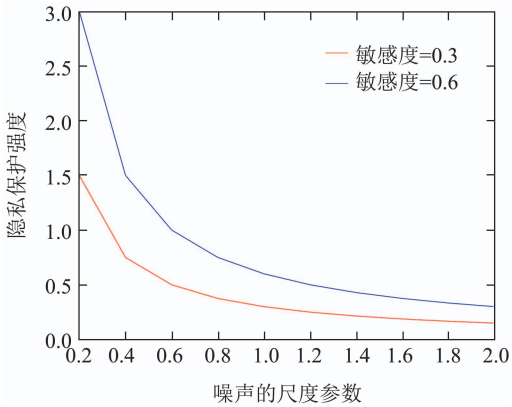


图 9 隐私保护强度

Fig. 9 The comparison of privacy protection strength

6 结论

本文研究了具有固定拓扑和切换拓扑结构的连续多智能体系统的隐私保护问题, 提出了具有隐私保护的多智能体系统协同控制算法, 应用矩阵论和概率统计对隐私保护协同控制算法的收敛性和隐私性进行理论分析, 得出了隐私泄漏对分布式协同控制闭环系统稳定性的影响, 最终该算法可以保护智能个体的数据隐私, 同时可以使得系统运动实现均方一致.

参考文献:

[1] HE J, CAI L, CHENG P, et al. Consensus-based data-privacy preserving data aggregation. *IEEE Transactions on Automatic Control*, 2019, 64(12): 5222 – 5229.

[2] DWORK C, ROTH A. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Ence*, 2013, 9(3/4): 211 – 407.

[3] HUANG Z, MITRA S, DULLERUD G. Differentially private iterative synchronous consensus. *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society*. New York: Association for Computing Machinery, 2012: 81 – 90.

[4] MO Y, MURRAY R M. Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, 2017, 62(2): 753 – 765.

[5] ERFAN N, PAVANKUMAR T, JORGE C. Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design. *Automatica*, 2017, 81(3): 221 – 231.

[6] GAO L, DENG S J, REN W. Differentially private consensus with an event-triggered mechanism. *IEEE Transactions on Control of Network Systems*, 2018, 6(1): 60 – 71.

[7] LÜ Y W, YANG G H, SHI C X. Differentially private distributed optimization for multi-agent systems via the augmented lagrangian algorithm. *Information Sciences*, 2020, 538(5): 39 – 53.

[8] YUAN Shuilian, PI Dechang, XU Meng. Trajectory privacy protection method based on differential privacy. *Acta Electronica Sinica*, 2021, 49(7): 1266 – 1273.
(袁水莲, 皮德常, 胥萌. 基于差分隐私的轨迹隐私保护方法. 电子学报, 2021, 49(7): 1266 – 1273.)

[9] CAI Jianping, LIU Ximeng, XIONG Jinbo, et al. Approximation method of multiple consistency constraint under differential privacy. *Journal on Communications*, 2021, 42(6): 107 – 117.
(蔡剑平, 刘西蒙, 熊金波, 等. 差分隐私下多重一致性约束问题的逼近方法. 通信学报, 2021, 42(6): 107 – 117.)

[10] WANG X, HE J, CHENG P, et al. Differentially private maximum consensus. *IFAC-PapersOnLine*, 2017, 50(1): 9509 – 9514.

[11] SHANG Yu, LIU Chenglin, CAO Kecai. Event-triggered consensus control of multi-agent systems under switching topologies. *Control Theory & Applications*, 2021, 38(10): 1522 – 1530.
(尚宇, 刘成林, 曹科才. 切换拓扑下多自主体系统的事件触发一致性控制. 控制理论与应用, 2021, 38(10): 1522 – 1530.)

[12] REN W, BEARD R W. Consensus seeking in multiagent systems under switchingally changing interaction topologies. *IEEE Transactions on Automatic Control*, 2005, 50(5): 655 – 661.

[13] WANG Fang, CHEN Xin, HE Yong, et al. Finite-time consensus control of second-order multi-agent systems with jointly-connected topologies. *Control Theory & Applications*, 2014, 31(7): 981 – 986.
(王芳, 陈鑫, 何勇, 等. 联合连通条件下的二阶多智能体系统有限时间一致性控制. 控制理论与应用, 2014, 31(7): 981 – 986.)

[14] PENG L, JIA Y. Consensus of a class of second-order multi-agent systems with time-delay and jointly-connected topologies. *IEEE Transactions on Automatic Control*, 2010, 55(3): 778 – 784.

[15] QIN J H, YU C B. Exponential consensus of general linear multi-agent systems under directed dynamic topology. *Automatica*, 2014, 50(9): 2327 – 2333.

[16] SU S Z, LIN Z L. Connectivity enhancing coordinated tracking control of multi-agent systems with a state-dependent jointly-connected dynamic interaction topology. *Automatica*, 2019, 101(12): 431 – 438.

[17] YU H, XIA H X. Adaptive consensus of multi-agents in networks with jointly connected topologies. *Automatica*, 2012, 48(8): 1783 – 1790.

[18] WANG F Y, YANG H Y, ZHANG S N. Containment control for first-order multi-agent systems with time-varying delays and uncertain topologies. *Communications in Theoretical Physics*, 2016, 66(8): 249 – 255.

作者简介:

孙玉娇 硕士研究生, 目前研究方向为多智能体编队控制, E-mail: syj944413542@163.com;

杨洪勇 博士, 教授, 目前研究方向为复杂网络、多自主体编队控制、智能控制和非线性系统同控制等, E-mail: hyyang@yeah.net;

于美妍 硕士研究生, 目前研究方向为多智能体编队控制, E-mail: ymyyumeiyan@163.com.