

谢光强, 胡明显, 李杨. 基于事件触发的多智能体系统差分隐私保护跟踪控制[J]. 广东工业大学学报, 2025, 42(2): 70–80. doi: 10.12052/gdutxb.240022.
Xie Guangqiang, Hu Mingyu, Li Yang. Event-triggered differential privacy protection tracking control[J]. Journal of Guangdong University of Technology, 2025, 42(2): 70–80. doi: 10.12052/gdutxb.240022.

基于事件触发的多智能体系统 差分隐私保护跟踪控制

谢光强, 胡明显, 李 杨

(广东工业大学 计算机学院, 广东 广州 510006)

摘要: 为了应对传统跟踪控制方法可能引起的窃听器攻击风险, 多智能体系统跟踪控制研究需要考虑隐私保护问题。本文在同时存在领导者与跟随者的多智能体系统中, 针对跟踪控制隐私保护问题, 提出了基于事件触发的分布式差分隐私保护跟踪控制方法(Event-triggered Distributed Differential Privacy Protection Tracking Control, EDPTC)。该方法旨在时刻保障领导者与跟随者的状态隐私, 同时实现均方跟踪。考虑到领导者与跟随者状态更新的差异, 基于敏感度上界定理, 分别设计了适应各自特点的隐私保护机制: 跟随者的递减噪声机制(The Decreasing Noise Mechanism of Followers, DNMF) 和领导者的随机噪声机制(The Random Noise Mechanism of Leaders, RNML)。此外, 为减少随机噪声对控制效果的影响, 引入领导者状态估计算法, 并设计分布式事件触发器以降低通信频率。通过矩阵分析和概率论, 证明了EDPTC的隐私性并推导出了其实现均方跟踪的充分条件。最后, 通过一系列数值仿真验证了方法的有效性。

关键词: 多智能体系统; 跟踪控制; 差分隐私保护; 事件触发

中图分类号: TP391

文献标志码: A

文章编号: 1007-7162(2025)02-0070-11

Event-triggered Differential Privacy Protection Tracking Control

Xie Guangqiang, Hu Mingyu, Li Yang

(School of Computer Science and Technology, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: To counter the risk of eavesdropper attacks inherent in traditional tracking control methods, research on tracking control in multi-agent systems must incorporate privacy protection considerations. This study introduces an event-triggered distributed differential privacy protection tracking control (EDPTC) method in multi-agent systems featuring both leaders and followers, aimed at addressing privacy protection issues in tracking control. The method is designed to ensure the privacy of the states of leaders and followers at all times while achieving mean square tracking. Given the differences in state updates between leaders and followers, privacy protection mechanisms tailored to each party are developed based on the sensitivity upper bound theorem: the decreasing noise mechanism for followers (DNMF) and the random noise mechanism for leaders (RNML). Moreover, to minimize the impact of random noise on control performance, a leader state estimation algorithm is introduced, and a distributed event trigger is designed to reduce the communication frequency. Additionally, through matrix analysis and probability theory, the privacy of the EDPTC is proven, and sufficient conditions for achieving mean square tracking are derived. Finally, a series of numerical simulations validate the effectiveness of the proposed method.

Key words: multi-agent system; tracking control; differential privacy protection; event-triggered strategy

多智能体系统协同控制强调通过智能体之间的协调和交互实现共同的目标, 已经得到了广泛的研

究^[1-4]。同时存在领导者与跟随者的多智能体系统作为多智能体系统协同控制的研究对象, 要求跟随者

收稿日期: 2024-02-05 录用日期: 2024-04-19 网络首发日期: 2024-08-28

基金项目: 国家自然科学基金资助项目(62006047, 618760439); 广东省重点研发项目(2021B0101220004)

作者简介: 谢光强(1979-), 男, 教授, 博士, 主要研究方向为多智能体、智能体控制, E-mail: xieqq@gdut.edu.cn

通信作者: 李杨(1980-), 女, 教授, 博士, 主要研究方向为多智能体、差分隐私保护, E-mail: liyang@gdut.edu.cn

根据领导者的指导执行任务或遵循特定的行为规范,这种分工方式能够更好地应对复杂、动态的任务和环境^[5]。跟踪控制作为同时存在领导者与跟随者的多智能体系统的研究热点和一致性控制的重要分支^[1],旨在使跟随者按照领导者的参考信号或轨迹进行变化,已广泛应用于编队控制^[6]、智能交通控制^[7]、智能网联汽车^[8]等领域。

多智能体系统的安全性是当前研究的重点,涉及到多种潜在的攻击者包括但不限于窃听者、诚实但好奇的智能体以及恶意智能体等^[9]。这些攻击者可能采用多种攻击手段,如DDos攻击、虚假信息注入攻击、差分攻击等^[9]。在多智能体系统安全领域,隐私保护问题尤为重要,吸引了众多学者的关注,研究重点在于如何防御可能导致隐私泄露的内部或外部攻击^[10]。由于传统的一致性控制协议通常假设智能体之间直接交换状态信息,所以其通信链路存在被攻击者窃听或实施差分攻击的风险,尤其是当智能体状态包含用户的敏感信息时^[10],这驱使研究人员探索了一些隐私保护机制^[11-16]。

差分隐私保护问题在多智能体系统的隐私保护研究中占据了重要地位,它主要探讨如何通过差分隐私噪声机制来确保智能体状态的隐私性。差分隐私^[11]由Dwork提出,其使用数学方法定义了一个严格且可量化的隐私保护模型。Huang等^[12]首次将差分隐私引入多智能体系统,提出了一个具有指数衰减的噪声机制。但是所设计的算法依赖于一个集中式服务器,因此其不适用于大规模的分布式多智能体系统。Nozari等^[13]提出了一个分布式差分隐私平均一致性算法,采用指数衰减的拉普拉斯噪声,可以在固定拓扑下保护智能体的初始状态,并且使用加噪机制混淆智能体状态,不会消耗太多计算资源。Gao等^[14]首次将事件触发机制加入差分隐私一致性算法中,在保证隐私的同时很好地提高了整个网络的执行效率。值得注意的是,上述算法大多使用指数衰减的噪声机制,只能提供对初始状态的隐私保护。因为指数级快速衰减的噪声会导致后续时刻状态的快速暴露,带来被攻击者揭示的危险,并且非指数递减的噪声机制意味着噪声参数将更复杂。因此,设计一个能够在任意时刻保护智能体状态的分布式差分隐私保护机制,是一个有挑战性且关键的问题,这成为了本文的动机之一。

在跟踪控制领域已有许多学者研究了隐私保护问题,Zha等^[15]将状态分解方法引入跟踪控制,提出了一种基于共识的立体信息滤波算法,可以保护局

部信息不被窃听者泄露。Gusrialdi^[16]研究了在通信网络和执行器存在恶意注入且同时存在窃听者时,如何达成弹性跟踪,提出了一个包含虚拟状态的分布式控制框架。尽管跟踪控制隐私保护领域已有众多研究,差分隐私保护方面却尚未见到有效的解决方案,相比于同态加密、状态分解等更复杂的隐私保护方法,差分隐私保护基于简单的加噪思想,能够在消耗不多计算资源的情况下,对智能体的状态提供有效的保护^[13]。差分隐私以其基于严格的数学模型定义和对抗强大攻击者的假设而闻名,它不仅能量化隐私保护等级^[11],还能为不同智能体提供不同强度的隐私保护,实现隐私保护的按需分配。因此,差分隐私保护在跟踪控制隐私保护领域显得尤为重要。在跟踪控制场景中,领导者和跟随者智能体在任何时刻都可能遭到潜在攻击者的窃听,这直接威胁到状态信息的隐私性。与大多数现有研究聚焦于平均一致性控制的差分隐私保护不同,跟踪控制差分隐私保护问题不仅需要关注跟随者的状态隐私性,还需考虑领导者的状态隐私性。此外,跟踪控制中智能体状态的更新方式与平均一致性控制存在显著差异,这要求为领导者和跟随者分别设计差分隐私噪声机制,这无疑增加了研究的挑战性。另一方面,提高通信效率是一致性控制领域的一个关键问题。分布式多智能体系统通常面临资源限制^[17],高通信效率通常意味着更高的任务执行效率。事件触发机制仅在特定事件发生时进行通信,能够显著提高通信效率^[18-20]。因此,本文的另一个研究动机是设计一种基于事件触发的跟踪控制方法,该方法包含能够时刻保护领导者和跟随者智能体状态的差分隐私噪声机制。

受以上背景驱动,本文研究了多智能体系统跟踪控制隐私保护问题,提出了一个分布式事件触发差分隐私保护跟踪控制方法(Event-triggered Distributed Differential Privacy Protection Tracking Control, EDPTC),能够时刻保护跟随者与领导者的状态并实现均方跟踪,并且通过事件触发机制提升了跟随者智能体的通信效率。具体的贡献点包括:

(1) 通过推导领导者与跟随者噪声机制对应的敏感度上界定理,提出了递减的跟随者噪声机制(The Decreasing Noise Mechanism of Followers, DNMF)与随机的领导者噪声机制(The Random Noise Mechanism of Leaders, RNML),相比于Nozari等的研究^[13],本文所提出的2种差分隐私噪声机制均采用非指数递减噪声,能够时刻对领导者与

跟随者的状态提供 ε -差分隐私的保护。

(2) 提出了一个分布式事件触发器,每个跟随者智能体只在特定事件时刻进行控制输入更新并与邻居交互,降低了通信频率,提升了系统的通信效率,相比于文献[14]的结果,本文探究了跟踪控制下的差分隐私保护机制与事件触发机制的融合。

1 预备知识与问题描述

1.1 代数图论与概率论

考虑一个离散线性且同时存在领导者与跟随者的多智能体系统,使用图 $G\{V, E\}$ 来表示跟随者的拓扑结构。 $V = \{1, \dots, N\}$ 表示 N 个跟随者智能体集合, $E\{(i, j) : i, j \in V, i \neq j\}$ 代表边集合, $(i, j) \in E$ 表示一条有向边,代表跟随者 j 能够收到跟随者 i 发送的信息。记跟随者 i 的邻居集合为 $N_i = \{j | (i, j) \in E, \forall j \in V\}$ 。如果 $(i, j) \in E$ 的同时必有 $(j, i) \in E$,则表示拓扑为无向图。 $A = [a_{ij}] \in \mathbf{R}^{N \times N}$ 代表跟随者邻接矩阵,当 $(i, j) \in E$ 时 $a_{ij} = 1$,其他情况 $a_{ij} = 0$ 。智能体 i 的度数表示为 $d_i = \sum_{j \in N_i} a_{ij}$, $K = \text{diag}(d_1, d_2, \dots, d_N)$ 为度矩阵。此外,图 G 的拉普拉斯矩阵定义为 $L = A - K$, $\lambda_{\max}(\cdot)$ 与 $\lambda_{\min}(\cdot)$ 分别代表矩阵的最大与最小特征值。

对于领导者,使用图 $G_0\{V_0, E_0\}$ 来表示其与跟随者的网络拓扑。领导者集合 $V_0 = \{0, \dots, N\}$,本文假设只存在一个领导者,标号为0。 $E_0\{(0, j) : j \in V\}$ 表示领导者与跟随者的边集合。图 G_0 对应的领导者邻接矩阵 $C = \text{diag}\{c_1, \dots, c_N\}$ 描述了领导者与跟随者的通信情况,其中当 $(0, i) \in E_0$ 时, $c_i = 1$,其他情况 $c_i = 0$ 。

对于一个服从拉普拉斯分布 $x \sim \text{Lap}(\mu, b)$ 的随机变量 x ,其均值 $E[x] = \mu$,方差 $V[x] = 2b^2$,并且 x 的概率密度函数表示为 $f(x) = \frac{1}{2b} e^{-\frac{|x-\mu|}{b}}$, $b > 0$ 。

1.2 离散时间跟踪控制

使用 $x_i(k)$ 表示第 i 个跟随者在 k 时刻的状态, $x_0(k)$ 为领导者的 k 时刻状态,其动力学方程如式(1)所示。

$$\begin{cases} x_i(k+1) = x_i(k) + u_i(k) \\ x_0(k+1) = x_0(k) + f(x_0(k)) \end{cases} \quad (1)$$

式中: $u_i(k)$ 为跟随者的控制输入。 $|f(x_0(k))| \leq \zeta$ 为有界的函数,其中 ζ 为正常数。在本文中,假设 $f(x_0(k)) \equiv 0$,故 $x_0(k) \equiv x_0(0)$,记为 x_0 。

1.3 攻击者模型

在本文中,潜在的攻击者被假设为窃听者。窃听者为熟悉网络拓扑结构并能够监听智能体通信信道

的外部攻击者。假设窃听者能持续监听智能体的外部可观测状态集合,定义为 $O_D(k) = \{\tilde{x}_0(k)S_0, \tilde{x}_1(k)S_1, \dots, \tilde{x}_N(k)S_N\}$,其中 $\tilde{x}_i(k)$ 为智能体 i 的 k 时刻状态外部可观测带噪状态,具体形式会在后文给出, S_i 为辅助参数,当智能体 i 需要向信道中发送状态信息时, $S_i = 1$,其他情况 $S_i = 0$ 。

相比于多智能体系统安全研究中讨论的其他攻击形式,例如诚实但好奇的节点、恶意信息注入者等^[15-16],本文所讨论的窃听者是一类可能构成更大威胁的攻击者,因为窃听者能够通过差分攻击还原出智能体的真实状态轨迹,尤其是在状态包含敏感信息时^[12]。此外,本文讨论的窃听者还包含了内部窃听者,其能够监听特定智能体的信道。图1展示了未考虑隐私保护的跟踪控制中窃听者对智能体状态隐私的威胁。

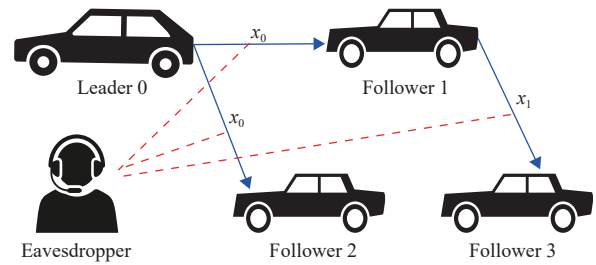


图1 窃听者监听信道并获取智能体状态信息
Fig.1 Eavesdropper listening to communication channels and obtaining state

1.4 定义与假设

首先,根据文献[14],因为差分隐私噪声的存在,本文的跟踪控制变为随机过程,故控制目标为统计学意义上的跟踪控制,即均方控制^[19]。

定义1^[19] 若对任意跟随者 i 和领导者0,在任意初始状态 $x_i(0)$ 与 x_0 下,其状态满足

$$\lim_{k \rightarrow +\infty} E[x_i(k) - x_0]^2 = 0 \quad (2)$$

则称系统实现了均方追踪控制。

接下来给出差分隐私理论相关的重要基础定义,包括临近状态向量、敏感度与差分隐私。其具体形式源自多智能体差分隐私保护研究^[21-22]。

定义2^[21] 如果多智能体系统的2个初始状态向量 $D = \{x_1(0), \dots, x_N(0)\}^T$ 与 $D' = \{x'_1(0), \dots, x'_N(0)\}^T$ 是邻近的,那么存在一个智能体 i_0 ,满足

$$\begin{cases} x_i(0) \neq x'_i(0), i = i_0 \\ x_i(0) = x'_i(0), i \neq i_0 \end{cases} \quad (3)$$

定义3^[21] 对于任意一对临近初始状态向量

D 与 D' ,隐私保护方法的敏感度定义如式(4)所示。

$$\Delta(k) = \sup \left\{ \frac{\|X_D(k) - X_{D'}(k)\|_1}{\|D - D'\|_1} \right\} \quad (4)$$

式中: $X_D(k) = \{x_1(k), \dots, x_N(k)\}^T$ 表示在初始状态 D 下智能体在 k 时刻的真实状态向量, $X_D(k)$ 与 $X_{D'}(k)$ 称为临近状态集, $\|\cdot\|_1$ 表示1范数。

定义4^[22] 噪声机制 M 在任意时刻 $k \geq 0$ 满足 ε -差分隐私,对任意一对临近状态向量 D 与 D' ,式(5)成立。

$$P\{O_D(k) \in O\} \leq e^{\varepsilon \|D - D'\|_1} P\{O_{D'}(k) \in O\} \quad (5)$$

式中: 可观测状态 $O_D(k) \in M(X_D(k))$, $\varepsilon > 0$ 代表隐私等级, $P\{\cdot\}$ 表示概率, $O \in \text{Range}(M)$ 是噪声机制值域的一个子集。

假设1 本文假设领导者与跟随者之间为单向通信,跟随者之间为双向通信。领导者0是全局可达的,即领导者与每个跟随者都存在一条路径。

假设2 控制增益 $\alpha(k)$ 满足

$$\sum_{k=0}^{\infty} \alpha(k) = \infty, \quad \sum_{k=0}^{\infty} \alpha^2(k) < \infty$$

1.5 问题描述

本文研究了分布式多智能体系统跟踪控制隐私保护问题,在同时存在领导者与跟随者的多智能体系统中,存在试图获取智能体真实状态的窃听者。本文的目标是设计一个分布式差分隐私事件触发跟踪控制方法,在对领导者与跟随者状态进行持续保护的前提下,设计一个事件触发器降低通信频率,并且最终能够实现均方跟踪。隐私保护的评判标准基于差分隐私,即是否能够防止攻击者几乎无法区分2个临近状态向量的可观测状态 $O_D(k)$ 与 $O_{D'}(k)$ 。

2 方法描述及分析

本节主要介绍了分布式事件触发差分隐私保护跟踪控制方法(Event-triggered Distributed Differential Privacy Protection Tracking Control, EDPTC),方法包含:(1) 控制输入更新协议;(2) 能够时刻保护跟随者与领导者状态隐私的噪声机制DNMF与RNML;(3) 有助于削弱随机噪声影响的领导者状态估计算法;(4) 分布式事件触发器。此外,说明了EDPTC方法的整体流程,并对EDPTC方法的隐私性和稳定性进行了分析和证明。

2.1 EDPTC方法

假设期望为所有智能体提供 ε -差分隐私的保护。每个跟随者智能体 i 在非事件触发时刻,控制输

入 $u_i(k)$ 将保持不变,但是在任意事件触发时刻 k_i 控制输入根据协议(6)更新 $u_i(k)$:

$$u_i(k_i) = \alpha(k_i) \left[\sum_{j \in N_i} a_{ij} (\tilde{x}_j(k_j) - x_i(k_i)) + c_i (\tilde{x}_0(k_i) - x_i(k_i)) \right] \quad (6)$$

式中: $\alpha(k_i)$ 为满足假设2的控制增益, $\tilde{x}_j(k_j)$ 为智能体 j 在距离 k_i 时刻最近的事件触发时刻 k_j 发送给邻居 i 的带噪状态, $x_i(k_i)$ 为智能体 i 在时刻 k_i 的状态,当领导者0与智能体 i 存在通信时 $c_i = 1$,其他情况 $c_i = 0$, $\tilde{x}_0(k_i)$ 为跟随者智能体 i 对领导者状态在 k_i 时刻的估计。

跟随者智能体 i 只有在特定事件触发时刻 k_i 才会给邻居发送信息,发送前,跟随者智能体 i 使用跟随者递减噪声机制式(7)混淆其真实状态:

$$\tilde{x}_i(k_i) = x_i(k_i) + \eta_i(k_i) \quad (7)$$

式中: $\eta_i(k_i)$ 为跟随者智能体 i 的噪声机制在 k_i 时刻产生的随机噪声,其服从拉普拉斯分布 $\text{Lap}(0, b_i(k))$, $b_i(k)$ 为时变拉普拉斯噪声参数,决定了 k 时刻的噪声强度,具体的参数设计过程会在隐私性分析小节中给出, $b_i(k)$ 设计如式(8)所示。

$$b_i(k) = \begin{cases} \frac{2}{\varepsilon}, & k = 0 \\ 2(1 - \alpha(k))b_i(k-1), & k \geq 1 \end{cases} \quad (8)$$

对于领导者0,因为其状态的更新方式与跟随者不同,因此为了时刻保护其状态,需要设计为固定参数 $b_0 = 2/\varepsilon$ 。领导者0使用领导者的随机噪声机制式(9)给其邻居跟随者发送带噪状态。

$$\tilde{x}_0(k) = x_0 + \eta_0(k) \quad (9)$$

式中: $\eta_0(k) \sim \text{Lap}(0, b_0)$ 。

因为领导者的噪声为非递减噪声,为了削减领导者噪声带来的负面影响,与领导者直接通信的跟随者智能体 i 使用领导者状态估计算法(10)来估计领导者的状态:

$$\tilde{x}_0(k) = \frac{\tilde{x}_0(k) + \sum_{m=0}^{k-1} \tilde{x}_0(m)}{k} \quad (10)$$

将式(6)与式(10)代入式(1)并根据式(7)展开,得到跟随者智能体的状态更新方程(11):

$$x_i(k_i + 1) = x_i(k_i) + \alpha(k_i) \left(\sum_{j \in N_i} a_{ij} \eta_j(k_j) + \frac{c_i}{k} \sum_{m=0}^k \eta_0(m) \right) + \alpha(k_i) \left[\sum_{j \in N_i} a_{ij} (x_j(k_j) - x_i(k_i)) + c_i (x_0(k_i) - x_i(k_i)) \right] \quad (11)$$

令噪声项 $\zeta_i(k) = \sum_{j \in N_i} a_{ij} \eta_j(k_j) + \frac{c_i}{k} \sum_{m=0}^k \eta_0(m)$, 记噪声向量为 $\zeta(k) = \{\zeta_1(k), \dots, \zeta_N(k)\}^T$, 状态向量为 $X(k) = \{x_1(k), \dots, x_N(k)\}^T$, 再记 $H = L + C$, 可得到式(11)在任意时刻 k 的矩阵形式(12):

$$X(k+1) = X(k) - \alpha(k) (H\hat{X}(k) - x_0 C \mathbf{1}) + \alpha(k) \zeta(k) \quad (12)$$

式中: $\hat{X}(k) = \{\hat{x}_1(k), \dots, \hat{x}_N(k)\}^T$, 且 $\hat{x}_i(k) = x_i(k_i^*)$, 其中 k_i^* 为跟随者智能体 i 距离时刻 k 的最近事件触发时刻。 $\mathbf{1}$ 为单位向量。通过定义测量误差与跟踪误差 $\delta_i(k) = x_i(k_i^*) - x_i(k)$, $e_i(k) = x_i(k_i^*) - x_0$, 并定义测量误差向量 $\delta(k) = \{\delta_1(k), \dots, \delta_N(k)\}^T$ 与跟踪误差向量 $e(k) = \{e_1(k), \dots, e_N(k)\}^T$, 式(12)可转换为误差矩阵式(13):

$$e(k+1) = e(k) - \alpha(k) (H(\delta(k) + e(k))) + \alpha(k) \zeta(k) \quad (13)$$

定义分布式事件触发器(14), 跟随者 i 只在触发如下事件的时刻更新控制输入 $u_i(k)$, 并给自己的邻居发送带噪状态 $\tilde{x}_i(k)$:

$$|\delta_i(k)| \geq \varphi |u_i(k)| \quad (14)$$

式中: $\varphi > 0$ 为事件触发参数, 具体将在定理3给出。

在0时刻所有跟随者智能体都会触发事件并初始化内存, 而在非0的 k 时刻, 跟随者 i 在EDPTC方法下的单次更新流程如下。

算法1 EDPTC方法下跟随者 i 在 k 时刻的单次更新流程。

- (1) 输入: 跟随者智能体 i 的状态 $x_i(k)$, 领导者0的带噪状态 $\tilde{x}_0(k)$, 事件触发参数 φ , 期望的隐私等级 ε 。
- (2) if 事件 $|\delta_i(k)| \leq \varphi |u_i(k)|$ 触发:
 - (a) if 领导者通信权值 $c_i \neq 0$: 根据估计算法(10)更新领导者状态估计 $\tilde{x}_0(k)$;
 - (b) 根据协议(6)更新控制输入 $u_i(k)$;
 - (c) 更新内存中的自身事件触发状态 $x_i(k_i)$, 将测量误差 $\delta_i(k)$ 重置为0;
 - (d) 根据式(8)计算拉普拉斯噪声参数 $b_i(k)$;
 - (e) 使用跟随者递减噪声机制DNMF(7)混淆真实状态并发送给邻居。
- (3) else: 保持 $u_i(k)$ 、内存不变, 不向邻居发送信息。
- (4) if 收到邻居智能体 j 的带噪状态 $\tilde{x}_j(k_j)$: 更新内存中的邻居最近事件触发带噪状态 $\tilde{x}_j(k_j)$ 。
- (5) 根据式(1)更新状态 $x_i(k+1)$ 。
- (6) 输出: 跟随者智能体 i 的下一时刻状态 $x_i(k+1)$ 。

此外, 注意本方法并未使用到任何全局信息, 因此是完全分布式的。

2.2 隐私性分析

本文方法是满足差分隐私的, 需要强调的是, 敏

感度描述了2个临近状态向量的差异, 根据文献[21], 设计一个差分隐私线性控制协议, 有必要从灵敏度的角度设计噪声参数。可以求出在满足差分隐私下, 噪声机制的敏感度上界, 从而反推出满足差分隐私所需的噪声参数。

定理1 在满足假设1、2的前提下, 当噪声机制DNMF与RNML满足差分隐私时, 其敏感度分别存在一个上界:

$$\sup_{k \geq 0} (\Delta(k)) \leq \begin{cases} 1, & k = 0, \\ \prod_{m=0}^{k-1} (1 - \alpha(m)), & k \geq 1 \end{cases} \quad (15)$$

$\sup_{k \geq 0} (\Delta_0(k)) \leq 1$, $\Delta(k)$ 与 $\Delta_0(k)$ 是跟随者递减噪声机制DNMF与领导者随机噪声机制RNML的敏感度。

证明 首先讨论跟随者递减噪声机制DNMF, 考虑极端情况, 即每个智能体在所有时刻都触发事件, 那么式(11)可改写为式(16):

$$x_i(k+1) = x_i(k) + \alpha(k) \left(\sum_{j \in N_i} a_{ij} \eta_j(k) + \frac{c_i}{k} \sum_{m=0}^k \eta_0(m) \right) + \alpha(k) \left[\sum_{j \in N_i} a_{ij} (x_j(k) - x_i(k)) + c_i (x_0(k) - x_i(k)) \right] \quad (16)$$

式中: k 为任意时刻。考虑2个临近状态向量, 在满足差分隐私的前提下, 其可观测状态与噪声机制是一致的, 故可得式(17):

$$x_i(k+1) - x'_i(k+1) = \left(1 - \alpha(k) \left(\sum_{j \in N_i} a_{ij} + c_i \right) \right) (x_i(k) - x'_i(k)) = \prod_{m=0}^k \left(1 - \alpha(m) \left(\sum_{j \in N_i} a_{ij} + c_i \right) \right) (x_i(0) - x'_i(0)) \quad (17)$$

当 $k = 0$ 时, 根据敏感度的定义可知, $\|X_D(0) - X_D'(0)\|_1 = \|D - D'\|_1$, 此时敏感度即为1。当 $k \geq 1$ 时, 推导式(18), 可以得到式(15)。

$$\begin{aligned} \|X_D(k) - X_D'(k)\|_1 &= \sum_i^N |x_i(k) - x'_i(k)| = \\ &= \sum_{i=1}^N \left| \prod_{m=0}^k \left(1 - \alpha(m) \left(\sum_{j \in N_i} a_{ij} + c_i \right) \right) (x_i(0) - x'_i(0)) \right| \leq \\ &= \sum_{i=1}^N \left| \prod_{m=0}^k (1 - \alpha(m)) (x_i(0) - x'_i(0)) \right| = \\ &= \prod_{m=0}^k (1 - \alpha(m)) \|D - D'\|_1 \end{aligned} \quad (18)$$

同理, 可以得到领导者随机噪声机制RNML的敏感度上界 $\sup_{k \geq 0} (\Delta_0(k)) \leq 1$, 证毕。

接下来说明EDPTC方法满足 ε -差分隐私的充分条件。

定理2 在满足假设1、2的前提下,假设期望的隐私等级 $\varepsilon > 0$,在任意 k 时刻,对任意跟随者 i 与领导者 0 ,当满足式(19):

$$b_i(k) \geq 2 \frac{\sup(\Delta(k)), k \geq 0}{\varepsilon}, b_0 \geq \frac{2}{\varepsilon} \quad (19)$$

噪声机制DNMF与RNML均满足 ε -差分隐私。

证明 首先对于跟随者递减噪声机制DNMF,使用 $f(O_D(k))$ 与 $f(O_{D'}(k))$ 分别表示2个临近状态向量对应的可观测状态的概率密度函数,定义 $\tilde{\mathbf{X}}(k) = \{\tilde{x}_1(k), \dots, \tilde{x}_N(k)\}^T$ 。因为在系统(1)中,唯一带来随机性的因素是拉普拉斯噪声,故有式(20):

$$\begin{aligned} f(O_D(k)) &= f(\tilde{\mathbf{X}}(k)) = f(\tilde{\mathbf{X}}(k)|\tilde{\mathbf{X}}(0), \tilde{\mathbf{X}}(1), \dots, \tilde{\mathbf{X}}(k-1)) = \\ &= f(\tilde{\mathbf{X}}(k)|\tilde{\mathbf{X}}(k-1)) = \prod_{i=1}^N f(\tilde{x}_i(k)|\tilde{x}_i(k-1)) = \\ &= \prod_{i=1}^N \text{Lap}(\tilde{x}_i(k) - x_i(k)) = \prod_{i=1}^N \frac{1}{2b_i(k)} \exp\left(-\frac{|\tilde{x}_i(k) - x_i(k)|}{b_i(k)}\right) \end{aligned} \quad (20)$$

其次,根据概率与概率密度函数的关系,可得式(21):

$$\frac{P\{O_D(k) \in O\}}{P\{O_{D'}(k) \in O\}} = \frac{f(O_D(k) \in O)}{f(O_{D'}(k) \in O)} = \frac{f(O_D(k))}{f(O_{D'}(k))} \quad (21)$$

式中: O 是噪声机制DNMF值域中的子集。对于任意时刻 $k \geq 0$,根据式(20)与式(21),推导得到式(22):

$$\begin{aligned} \frac{f(O_D(k))}{f(O_{D'}(k))} &= \prod_{i=1}^N \frac{\text{Lap}(\tilde{x}_i(k) - x_i(k))}{\text{Lap}(\tilde{x}_i(k) - x'_i(k))} = \\ &= \prod_{i=1}^N \frac{\exp\left(-\frac{|\tilde{x}_i(k) - x_i(k)|}{b_i(k)}\right)}{\exp\left(-\frac{|\tilde{x}_i(k) - x'_i(k)|}{b_i(k)}\right)} \leq \\ &= \prod_{i=1}^N \exp\left(\frac{|\tilde{x}_i(k) - x_i(k) - \tilde{x}_i(k) + x'_i(k)|}{b_i(k)}\right) \leq \\ &= \prod_{i=1}^N \exp\left(\frac{|\tilde{x}_i(k) - \tilde{x}_i(k)| + |x_i(k) - x'_i(k)|}{b_i(k)}\right) \leq \\ &= \exp\left(\sum_{i=1}^N \frac{2|x_i(k) - x'_i(k)|}{b_i(k)}\right) \end{aligned} \quad (22)$$

又因为 $\|\mathbf{X}_D(k) - \mathbf{X}_{D'}(k)\|_1 = \sum_{i=1}^N |x_i(k) - x'_i(k)|$,同时代入 $b_i(k) \geq 2 \sup_{k \geq 0}(\Delta(k))/\varepsilon$,可以得到式(23):

$$\begin{aligned} \frac{f(O_D(k))}{f(O_{D'}(k))} &\leq \exp\left(\frac{\varepsilon \|\mathbf{X}_D(k) - \mathbf{X}_{D'}(k)\|_1}{\sup_{k \geq 0} \Delta(k)}\right) \leq \\ &\leq \exp(\varepsilon \times \|\mathbf{D} - \mathbf{D}'\|_1) \end{aligned} \quad (23)$$

根据式(21)与(23),可得最终形式(24):

$$P\{O_D(k) \in O\} \leq e^{\varepsilon \times \|\mathbf{D} - \mathbf{D}'\|_1} P\{O_{D'}(k) \in O\} \quad (24)$$

而对于领导者的随机噪声机制RNML,其分析与DNMF类似,故证毕。

2.3 收敛性分析

在本节中,将分析EDPTC方法的收敛性,给出系统达成均方跟踪的充分条件。首先,给出如下2个引理:

引理1^[23] 0 是拉普拉斯矩阵 $\mathbf{L}$ 的一个特征值,对应特征向量为 $\mathbf{1}$,并且所有的非 0 特征值都有正实部。此外,图 G 包含一棵生成树当且仅当 0 是 $\mathbf{L}$ 的一个简单特征值。

引理2^[24] 当且仅当领导者 0 全局可达,存在一个正定矩阵 $\mathbf{P}$ 满足式(25):

$$\mathbf{P}\mathbf{H} + \mathbf{H}^T \mathbf{P} = \mathbf{I} \quad (25)$$

式中: $\mathbf{H} = \mathbf{L} + \mathbf{C}$, $\mathbf{I}$ 为单位矩阵。

定理3 在满足假设1、2的前提下,当事件触发参数 $\varphi < 1/\lambda_{\max}(\mathbf{H}^T \mathbf{P}\mathbf{H})$ 时,EDPTC方法能够达成均方跟踪。

证明 根据误差矩阵式(13),定义能量函数为

$$\mathbf{V}(k) = \mathbf{E}[\mathbf{e}^T(k) \mathbf{P} \mathbf{e}(k)] \quad (26)$$

式中: $\mathbf{P}$ 为满足式(25)的正定矩阵,将 $\mathbf{V}(k+1)$ 展开,可得式(27)。

$$\begin{aligned} \mathbf{V}(k+1) &= \mathbf{E}[\mathbf{e}^T(k+1) \mathbf{P} \mathbf{e}(k+1)] = \\ &= \mathbf{E}[\mathbf{e}^T(k) (\mathbf{P} - \alpha(k) \mathbf{H}^T \mathbf{P}) (\mathbf{I} - \alpha(k) \mathbf{H}) \mathbf{e}(k)] + \\ &= \alpha^2(k) \mathbf{E}[\delta^T(k) \mathbf{H}^T \mathbf{P} \mathbf{H} \delta(k)] + \alpha^2(k) \mathbf{E}[\zeta^T(k) \mathbf{P} \zeta(k)] = \\ &= \mathbf{E}[\mathbf{e}^T(k) \mathbf{P} \mathbf{e}(k)] - \alpha(k) \mathbf{E}[\|\mathbf{e}(k)\|^2] + \\ &= \alpha^2(k) \mathbf{E}[\mathbf{e}^T(k) \mathbf{H}^T \mathbf{P} \mathbf{H} \mathbf{e}(k)] + \alpha^2(k) \mathbf{E}[\delta^T(k) \mathbf{H}^T \mathbf{P} \mathbf{H} \delta(k)] + \\ &= \alpha^2(k) \mathbf{E}[\zeta^T(k) \mathbf{P} \zeta(k)] \end{aligned} \quad (27)$$

式中: $\|\cdot\|$ 表示2范数,化简利用了 $\mathbf{P}\mathbf{H} + \mathbf{H}^T \mathbf{P} = \mathbf{I}$ 。再根据矩阵谱定理,可得式(28)。

$$\begin{cases} \lambda_{\min}(\mathbf{P}) \mathbf{V}(k) \leq \mathbf{E}[\|\mathbf{e}(k)\|^2] \\ \lambda_{\max}(\mathbf{P}) \mathbf{E}[\|\zeta(k)\|^2] \geq \mathbf{E}[\zeta^T(k) \mathbf{P} \zeta(k)] \\ \lambda_{\max}(\mathbf{H}^T \mathbf{P} \mathbf{H}) \mathbf{V}(k) \geq \mathbf{E}[\mathbf{e}^T(k) \mathbf{H}^T \mathbf{P} \mathbf{H} \mathbf{e}(k)] \\ \lambda_{\max}(\mathbf{H}^T \mathbf{P} \mathbf{H}) \mathbf{E}[\|\delta(k)\|^2] \geq \mathbf{E}[\delta^T(k) \mathbf{H}^T \mathbf{P} \mathbf{H} \delta(k)] \end{cases} \quad (28)$$

记 $J_0 = \lambda_{\min}(\mathbf{P})$, $J_1 = \lambda_{\max}(\mathbf{P})$ 且 $J_2 = \lambda_{\max}(\mathbf{H}^T \mathbf{P} \mathbf{H})$,根据引理1,它们都为常数。将它们代入式(27),可得式(29)。

$$\begin{aligned} \mathbf{V}(k+1) &\leq (1 - \alpha(k) J_0 + \alpha^2(k) J_2) \mathbf{V}(k) + \\ &+ \alpha^2(k) (J_2 \mathbf{E}[\|\delta(k)\|^2] + J_1 \mathbf{E}[\|\zeta(k)\|^2]) \end{aligned} \quad (29)$$

对于 $E\|\delta(k)\|^2$ 项,因为每当事件 $|\delta_i(k)| \geq \varphi|u_i(k)|$ 触发都会重置 $\delta_i(k) = 0$,故 $|\delta_i(k)|$ 存在上界,结合 $\varphi < 1/\lambda_{\max}(\mathbf{H}^T \mathbf{P} \mathbf{H}) = 1/J_2$,进而可得式(30)。

$$\|\delta(k)\| < \alpha(k)\varphi\|\mathbf{H}\mathbf{e}(k)\| < \frac{\alpha(k)\|\mathbf{H}\|}{J_2}\|\mathbf{e}(k)\| \quad (30)$$

对式(30)两边同时取均方,可得式(31)。

$$E\|\delta(k)\|^2 < \frac{\|\mathbf{H}\|}{J_2}E\|\mathbf{e}(k)\|^2 \leq \frac{\|\mathbf{H}\|}{J_2}\lambda_{\max}(\mathbf{P})V(k) \quad (31)$$

对于 $E\|\zeta(k)\|^2$,可推导得到式(32):

$$\begin{aligned} E\|\zeta(k)\|^2 &= \sum_{i=1}^N E\left(\sum_{j \in N_i} a_{ij}\eta_j(k_j) + \frac{c_i}{k} \sum_{m=0}^k \eta_0(m)\right)^2 = \\ &\sum_{i=1}^N \left(\sum_{j \in N_i} a_{ij}^2 E[\eta_j^2(k_j)] + \frac{c_i^2}{k^2} \sum_{m=0}^k E[\eta_0^2(m)]\right) \leq \frac{2N^2}{\varepsilon^2} + \frac{2Nc_i^2}{k\varepsilon^2} \end{aligned} \quad (32)$$

其中放缩使用了拉普拉斯噪声的期望为0,即 $E[\eta_j(k)] = E[\eta_0(k)] = 0$,并且使用了拉普拉斯分布性质 $E[\eta_j^2(k)] = 2b_j^2(k) \leq \frac{2}{\varepsilon^2}$, $E[\eta_0^2(k)] = 2b_0^2 = \frac{2}{\varepsilon^2}$ 。

将式(31)与(32)代入(29),可得式(33)。

$$\begin{aligned} V(k+1) &< (1 - \alpha(k)J_0 + \alpha^2(k)J_2 + \alpha^3(k)J_3)V(k) + \\ &\alpha^2(k)J_1 \left(\frac{2N^2}{\varepsilon^2} + \frac{2Nc_i^2}{k\varepsilon^2}\right) \end{aligned} \quad (33)$$

式中: $J_3 = \lambda_{\max}(\mathbf{P})\|\mathbf{H}\|$ 为常数。根据假设2, $\lim_{k \rightarrow +\infty} \alpha^q(k) = 0$, $q \geq 0$ 。对式(33),两边同时取 $k \rightarrow +\infty$,可得式(34)。

$$V(k+1) < V(k) \quad (34)$$

又因为 $V(k) = E[\mathbf{e}^T(k)\mathbf{P}\mathbf{e}(k)] \geq 0$,故当 $k \rightarrow +\infty$ 时 $V(k) \rightarrow 0$ 。故式(35)成立:

$$\lim_{k \rightarrow +\infty} E\|\mathbf{e}(k)\|^2 = \lim_{k \rightarrow +\infty} \sum_{i=1}^N E[x_i(k) - x_0]^2 = 0 \quad (35)$$

此时系统达成均方跟踪,证毕。

注解1 因为本文研究的是离散时间多智能体系统,最坏情况下,事件触发器会在所有时刻触发,但是不会无限触发,所以可以排除芝诺行为。

3 实验分析

3.1 仿真设置

考虑一个包含单个领导者0与4个跟随者{1,2,3,4}的多智能体系统,其拓扑结构如图2所示,为了更客观地讨论,与Hu等的研究^[24]使用相同的拓扑。显然领导者0是全局可达的,满足假设1。

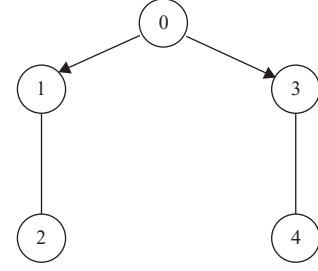


图2 拓扑图
Fig.2 Topology

假设智能体的初始状态分别为 $x_0 = 0$, $\mathbf{X}(0) = \{-12, -5, 8, 10\}^T$, 控制增益设置为 $\alpha(k) = 1/(1+k)^{0.6}$, 显然满足假设2。进行简单的计算,可以求出拓扑对应的矩阵 $\mathbf{H}$ 与 $\mathbf{P}$:

$$\left\{ \begin{aligned} \mathbf{H} &= \begin{bmatrix} 2 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 2 & -1 \\ 0 & 0 & -1 & 1 \end{bmatrix} \\ \mathbf{P} &= \begin{bmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.5 & 1 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 \\ 0 & 0 & 0.5 & 1 \end{bmatrix} \end{aligned} \right. \quad (36)$$

可以求出 $\lambda_{\max}(\mathbf{H}^T \mathbf{P} \mathbf{H}) = 1.31$, 故设置 $\varphi = 0.7 < 1/1.31$, 满足定理3。对于领导者随机噪声机制RNML与跟随者递减噪声机制DNMF, 均给定期望隐私等级 $\varepsilon = 1$ 。此外, 注意本文假设领导者唯一, 故领导者可观测状态 $O_D(k) = \tilde{x}_0(k)$ 。

3.2 收敛性验证

图3展示了跟随者在 $0 \leq k \leq 200$ 离散时刻内的状态轨迹 $\mathbf{X}(k)$, 使用“+”号来标记领导者0的状态 x_0 , 可以看到所有跟随者都能够成功跟踪领导者, 验证了方法的有效性。

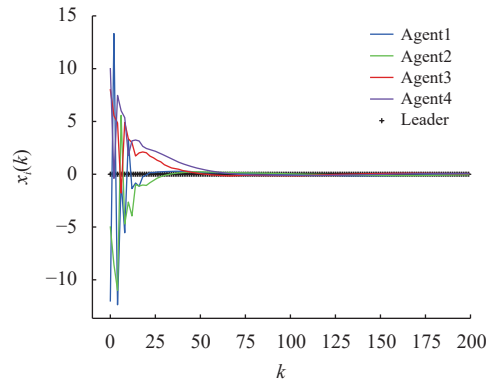


图3 状态轨迹
Fig.3 State trajectory

因为拉普拉斯噪声具有随机性,故需要进行多次重复实验来验证方法的有效性。图4说明了跟随者在10 000次相同条件的重复实验下的均方跟踪误差 $E[x_i(k) - x_0]^2$, 其代表了跟随者与领导者智能体状态在统计学意义上的差值。可以观测到随着时间推移, 所有跟随者智能体的均方跟踪误差都趋于0, 这与定理3相符合。

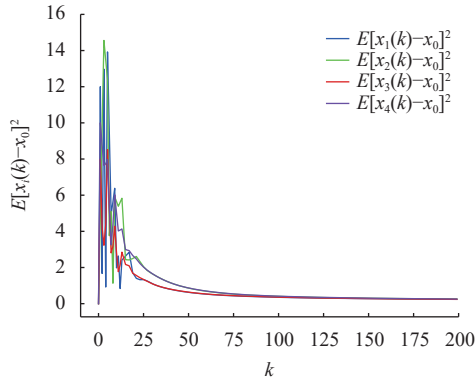


图4 均方误差轨迹

Fig.4 Mean squared error trajectory

3.3 事件触发分析

在EDPTC方法中设计了事件触发器(14), 在本小节将验证其能够显著提升跟随者智能体之间的通信效率。根据定理3, 事件触发参数 φ 在满足 $\varphi < \lambda_{\max}(\mathbf{H}^T \mathbf{P} \mathbf{H})$ 时, 系统能够达成均方跟踪。图5表示在单次仿真实验下跟随者智能体的事件触发时刻图, 其分别说明了跟随者智能体{1,2,3,4}在时间区间 $0 \leq k \leq 100$ 内的事件触发情况, 使用不同颜色的“x”号来表示不同智能体的事件触发, 黑色实心点代表离散时刻。可以看到跟随者智能体并不会在所有时刻触发事件, 而只在满足特定事件 $|\delta_i(k)| \geq \varphi|u_i(k)|$ 的时刻触发事件, 从而避免了连续通信, 提升了通信效率。

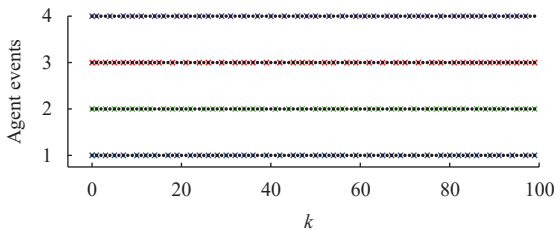


图5 跟随者智能体事件触发时刻

Fig.5 Follower agent event time

图6说明了跟随者智能体1的测量误差绝对值 $|\delta_1(k)|$ 与事件触发阈值 $\varphi|u_1(k)|$ 在时间区间 $0 \leq k \leq 100$ 内的轨迹, 可以看到跟随者智能体1的测量误差绝对值在大于等于事件触发阈值时, 即 $|\delta_1(k)| \geq \varphi|u_1(k)|$

时会触发事件, 并重置测量误差 $\delta_1(k)$ 为0, 因为根据定义 $\delta_i(k) = x_i(k_i^*) - x_i(k)$, 测量误差为跟随者智能体在 k 时刻状态与最近事件触发时刻状态的差值。

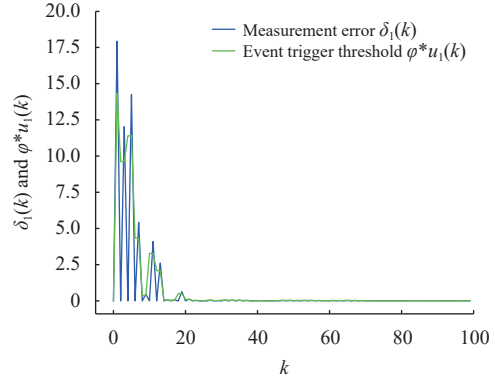


图6 跟随者智能体1的跟踪误差与事件触发阈值轨迹

Fig.6 Tracking error and event trigger threshold trajectory of follower agent 1

表1展示了跟随者智能体在 $0 \leq k \leq 100$ 时间区间下的事件触发次数统计, 跟随者智能体在 $0 \leq k \leq 100$ 时间区间下平均事件触发次数为30.25次。相比于未使用事件触发机制的跟踪控制方法, EDPTC方法下跟随者智能体不会在每一离散时刻都与邻居进行通信, 而只在事件触发时刻与邻居进行通信。这意味着跟随者智能体平均通信次数减少了69.75%, 故所提出的事件触发器大大减少了跟随者智能体之间的通信次数, 提升了跟随者智能体的通信效率。

表1 事件触发次数统计
Table 1 The statistics of event times

Agent	Event Times	Total Times	Rate/%
1	29	100	29
2	30	100	30
3	31	100	31
4	31	100	31

图7是控制输入 $u_i(k)$ 的轨迹, 根据EDPTC方法, 跟随者智能体只有在事件触发时刻才更新控制输入 $u_i(k)$, 其余时刻保持 $u_i(k)$ 不变, 即说明了所提出的事件触发机制能够避免控制输入的频繁更新。可以看到, 控制输入 $u_i(k)$ 的轨迹为直线时即是非事件触发时刻, 此时不更新 $u_i(k)$, 否则 $u_i(k)$ 的曲线将进行一次跳变。此外, 因为均方跟踪的达成, 可以观察到最终所有跟随者智能体的控制输入都趋近于0。

3.4 隐私性验证

本节将验证EDPTC方法的差分隐私性, 并分别说明2种噪声机制DNMF与RNML的运作细节。为了更好地分析隐私性, 设置 $\mathbf{X}(0)$ 的临近初始状态向

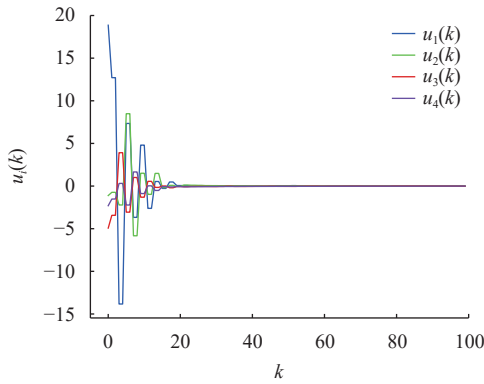


图7 控制输入轨迹

Fig.7 Control input trajectory

量 $X'(0) = \{-11, -5, 8, 10\}^T$, 显然 $\|X(0) - X'(0)\|_1 = \|D - D'\|_1 = 1$, 类似的, 给定 x_0 的临近状态 $x'_0 = 1$ 。根据差分隐私的定义, 更小的隐私等级绝对值 $|\varepsilon|$ 意味着更强的隐私保护水平, 攻击者将更难区分2个临近状态向量。参考文献[22], 通过式(37)能够估测出噪声机制的隐私等级, 其中 $Q(k) \in \text{Range}(M)$ 是噪声机制值域中的一个时变集合。用于估计跟随者噪声机制DNMF的 $Q(k)$ 具体如式(38)所示。

$$\varepsilon(k) = \frac{\ln(P\{O_D(k) \in Q(k)\})}{\ln(P\{O_{D'}(k) \in Q(k)\})} \quad (37)$$

$$\{Q(k)\}_{k=0}^{+\infty} = \{\xi \in \text{Range}(M) : 18 \times 0.975^k \leq \|\xi\|_F \leq 18\}_{k=0}^{+\infty} \quad (38)$$

式中: $\|\cdot\|_F$ 表示矩阵的斐波那契范数。用于估计领导者噪声机制RNML的 $Q(k)$ 具体如式(39)所示。

$$\{Q(k)\}_{k=0}^{+\infty} = \{\xi \in \text{Range}(M) : 0 \leq \|\xi\|_F \leq 1\}_{k=0}^{+\infty} \quad (39)$$

需要强调的是, 因为差分隐私定义的任意性, 找到一个能够完全准确估测隐私等级的集合 $Q(k)$ 是困难的, 但是通过定义一个较严格的集合, 可以确保估测出的 $|\varepsilon(k)| \leq \varepsilon$ 。

为了说明EDPTC方法的优越性, 本文方法将与Nozari等[13]提出的方法中使用的指数递减差分隐私噪声机制(以下简称为Nozari2018)进行对比, 其具体的参数设置与文献[13]的第6节保持一致。考虑在跟随者噪声机制中使用文献[13]中指数递减的时变拉普拉斯参数 $b_i(k) = c_i q_i^k$ 代替式(8), 其他设置均与EDPTC方法相同, 并且同样使用式(38)作为跟随者噪声机制的隐私等级估测集合。为了排除干扰, 2个对比方法均不使用领导者噪声机制, 即领导者状态不加噪。图8展示了EDPTC方法与Nozari2018的跟随者噪声机制的估测隐私等级对比图。由图8所示,

EDPTC方法中的DNMF噪声机制能够时刻对跟随者的状态提供 ε -差分隐私的保护, 而Nozari2018只能保护跟随者智能体的初始状态, 而在其余时刻临近状态向量的差异为无限大, 无法实现 ε -差分隐私, 故无法保护初始时刻以外的跟随者智能体状态。

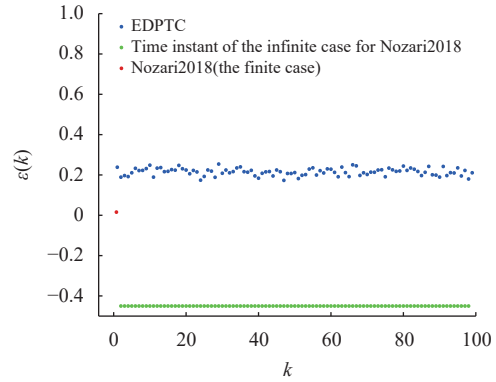


图8 EDPTC与Nozari2018的隐私等级估测轨迹对比

Fig.8 Comparison of privacy level estimation trajectories between EDPTC and Nozari2018

为了说明所提出的方法能够提供用户期望的隐私等级, 图9分别展示了跟随者与领导者使用的噪声机制DNMF与RNML在给定期望隐私等级 $\varepsilon = 1$ 与 $\varepsilon = 2$ 下, 在时间区间 $0 \leq k \leq 100$ 内隐私等级的估测轨迹, 可以看到其能够时刻提供 ε -差分隐私的保护, 并且可以根据给定的隐私等级调整隐私保护强度, 这验证了定理2。

为了说明领导者随机噪声机制RNML与跟随者递减噪声机制的区别, 图10分别说明了领导者0与跟随者1在时间区间 $0 \leq k \leq 100$ 下的带噪状态与真实状态轨迹。跟随者 i 在事件触发时刻 k_i , 将使用噪声机制式(7)给邻居发送带噪状态 $\tilde{x}_i(k_i)$, 其余时刻保持静默。图10(b)中, 蓝色实线代表智能体1的真实状态轨迹 $x_1(k)$, 红色散点代表1发送给其邻居的带噪状态 $\tilde{x}_1(k_i)$, 因为事件触发器的存在, $\tilde{x}_1(k_i)$ 并不是连续的, 并且 $\tilde{x}_1(k_i)$ 逐渐收敛至 $x_1(k)$ 。图10(a)为领导者0的真实状态 x_0 与其根据噪声机制式(9)发送给邻居的带噪状态 $\tilde{x}_0(k)$, 因为使用了非递减的拉普拉斯噪声, $\tilde{x}_0(k)$ 的均方为 x_0 , 但轨迹并不会收敛至 x_0 。

4 结论

本文研究了离散线性且同时存在领导者与跟随者的多智能体系统的跟踪控制隐私保护问题, 提出了一个差分隐私事件触发跟踪控制方法EDPTC。本方法不仅考虑了隐私保护问题, 还设计了一个分布式事件触发器。能够时刻保护跟随者与领导者的状

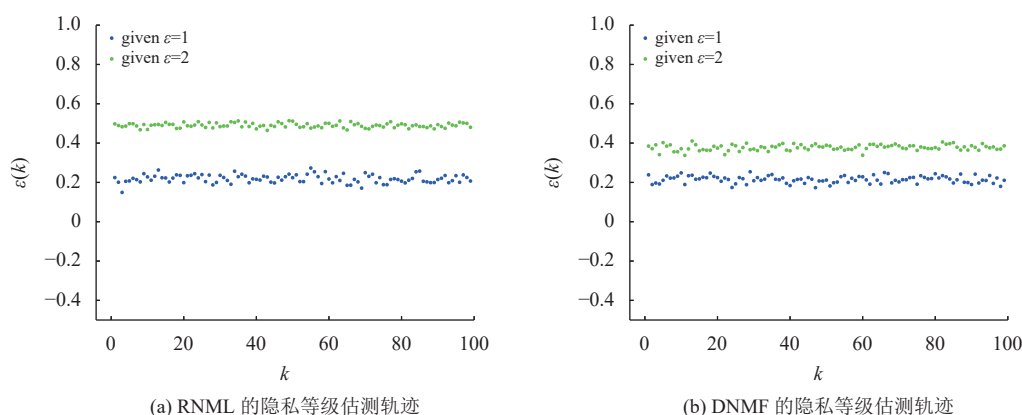


图9 RNML与DNMF的隐私等级估测轨迹

Fig.9 Privacy Level Estimation Trajectory of RNML and DNMF

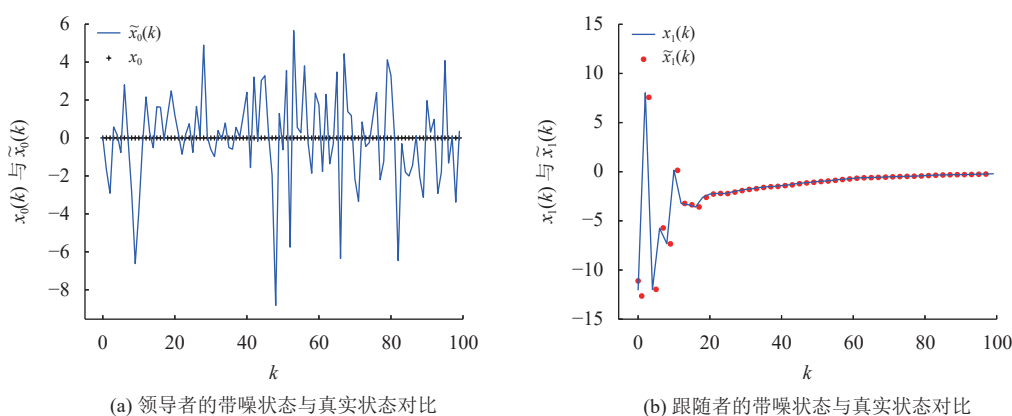


图10 领导者与跟随者的带噪状态与真实状态

Fig.10 The noisy and real states of leaders and followers

态不被窃听者还原,且能够提供期望的隐私保护水平,并通过事件触发机制降低了跟随者之间的通信频率。具体来说,EDPTC方法具有如下优点:(1)能够时刻对领导者与跟随者的状态提供期望等级的差分隐私保护;(2)方法是完全分布式的,且得益于领导者状态估计算法,能够实现均方跟踪;(3)所提出的事件触发器能够降低通信频率。未来的工作将讨论在切换拓扑场景下的跟踪控制隐私保护问题。

参考文献:

- [1] AMIRKHANI A, BARSHOOI AH. Consensus in multi-agent systems: a review [J]. *Artificial Intelligence Review*, 2022, 55(5): 3897-3935.
- [2] WANG S, WAN J, ZHANG D, *et al.* Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination [J]. *Computer Networks*, 2016, 101: 158-168.
- [3] XIE G, XU H, LI Y, *et al.* Fast distributed consensus seeking in large-scale and high-density multi-agent systems with connectivity maintenance [J]. *Information Sciences*, 2022, 608: 1010-1028.
- [4] MAZZARINO P R, MACII A, BOTTACCIOLI L, *et al.* A multi-agent framework for smart grid simulations: strategies for power-to-heat flexibility management in residential context [J]. *Sustainable Energy, Grids and Networks*, 2023, 34: 101072.
- [5] HONG Y, CHEN G, BUSHNELL L. Distributed observers design for leader-following control of multi-agent networks [J]. *Automatica*, 2008, 44(3): 846-850.
- [6] AZARBAHRAM A, AMINI A, PARIZ N. Event-triggered tracking formation of networked nonlinear intelligent transportation systems surrounded by random disturbances [J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(11): 21959-21970.
- [7] BALBO F, MANDIAU R, ZARGAYOUNA M. Extended review of multi-agent solutions to advanced public transportation systems challenges[J]. *Public Transport*, 2024, 16: 1-28.
- [8] 谢光强, 赵俊伟, 李杨, 等. 基于多集群系统的车辆协同换道控制[J]. *广东工业大学学报*, 2021, 38(5): 1-9.

XIE G Q, ZHAO J W, LI Y, *et al.* Cooperative lane-chan-

