(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115185189 B
(45)授权公告日 2023.09.05

(21)申请号 202211081802.0
(22)申请日 2022.09.06
(65)同一申请的已公布的文献号
申请公布号 CN 115185189 A
(43)申请公布日 2022.10.14
(73)专利权人 人工智能与数字经济广东省实验室(广州)
地址 510330 广东省广州市海珠区新港东路2429号首层自编051房
(72)发明人 张银炎 邓青云
(74)专利代理机构 广州科粤专利商标代理有限公司 44001
专利代理师 劳剑东 邓潮彬
(51)Int.Cl.
G05B 13/04(2006.01)

(56)对比文件
CN 113312635 A,2021.08.27
CN 108803349 A,2018.11.13
CN 111781822 A,2020.10.16
CN 114510730 A,2022.05.17
CN 110782011 A,2020.02.11
CN 114545773 A,2022.05.27
US 2020177366 A1,2020.06.04
Qingyun Deng .etal.Distributed Near-Optimal Consensus of Double-Integrator Multi-Agent Systems With Input Constraints.《2021 International Joint Conference on Neural Networks (IJCNN)》.2021,第1-6页.

审查员 焦雅楠

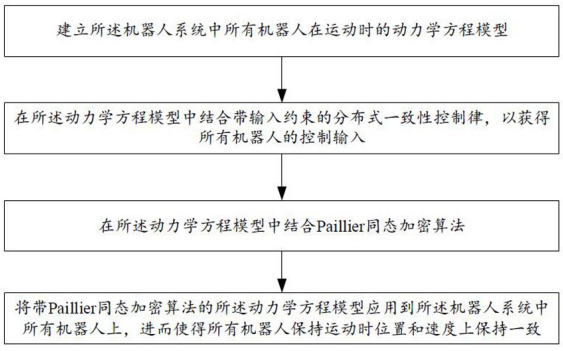
权利要求书6页 说明书13页 附图3页

(54)发明名称

带隐私保护的一致性最优控制方法、系统、设备和介质

(57)摘要

本发明公开了一种带隐私保护的一致性最优控制方法,涉及控制领域和机器人领域,所述方法包括:建立所述机器人系统中所有机器人在运动时的动力学方程模型;在所述动力学方程模型中结合带输入约束的分布式一致性控制律,以获得所有机器人的控制输入;在所述动力学方程模型中结合Paillier同态加密算法;将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上,进而使得所有机器人保持运动时位置和速度上保持一致。本发明可以让所有机器人最终在位置和速度上保持一致,同时避免泄露私有信息。



CN 115185189 B

1.一种带隐私保护的一致性最优控制方法,应用于机器人系统,其特征在于,包括如下步骤:

建立所述机器人系统中所有机器人在运动时的动力学方程模型;

在所述动力学方程模型中结合带输入约束的分布式一致性控制律,以获得所有机器人的控制输入;

在所述动力学方程模型中结合Paillier同态加密算法;

将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上,进而使得所有机器人保持运动时位置和速度上保持一致;

所述动力学方程模型具体为:

设无关质量因素的机器人在一维直线上运动,且每个机器人与系统中的部分或全部机器人通信,利用机器人的位置,速度,控制输入和控制输出建立机器人的双积分器动力学方程,具体的,

设机器人具有如下双积分器动力学方程:

$$\begin{cases}\dot{\mathbf{x}}=\mathbf{v}\\ \dot{\mathbf{v}}=\mathbf{u}\\ \mathbf{y}=\mathbf{x}\end{cases}$$

其中$x=[x_1,x_2\cdots x_n]^T$,$v=[v_1,v_2\cdots v_n]^T$表示各个机器人们的状态向量,$u=[u_1,u_2\cdots u_n]^T$,$y=[y_1,y_2\cdots y_n]^T$分别表示各个机器人的状态向量输入向量和输出向量,对于第i个机器人x_i,v_i,u_i,y_i分别代表其位置,速度,控制输入和控制输出;

设无关质量因素的机器人在二维平面上和三维空间上运动,且每个机器人与系统中的部分或全部机器人通信,利用机器人的位置,速度,控制输入和控制输出建立机器人的双积分器动力学方程,具体的,先分别计算各二维、三维坐标轴方向对应的控制输入值,然后矢量合成为一个方向的控制输入值,最终让每个机器人的位置达到一致;

所述带输入约束的分布式一致性控制律,具体为:

借助如下积分型性能指标

$$J_{\mathrm{d}}(t)=\int_0^T\mathbf{y}^{\mathrm{T}}(t+\tau)L\mathbf{y}(t+\tau)\mathrm{d}\tau$$

其中L是多智能体系统对应拓扑图的拉普拉斯矩阵,T称为预测间隔,得到如下优化问题

$\min\ J_d(t)$

$$\text{subject to}\ \ \dot{\mathbf{x}}=\mathbf{v}$$

$$\dot{\mathbf{v}}=\mathbf{u}$$

$y=x$

$u\in\Omega$

其中Ω是一个关于输入的闭合凸集合,约定了输入的上下界,通过泰勒展开

$$\mathbf{y}(t+\tau)\approx\mathbf{y}(t)+\tau\dot{\mathbf{y}}(t)+\frac{\tau^2}{2}\ddot{\mathbf{y}}(t)$$

$$=\mathbf{x}(t)+\tau\mathbf{v}(t)+\frac{\tau^2}{2}\mathbf{u}(t).$$

代入上述优化问题，经过简化及省略与输入u无关的部分，得到剩余

$$\Phi=\frac{T^5}{20}\mathbf{u}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^4}{4}\mathbf{v}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^3}{3}\mathbf{x}^{\mathrm{T}}(t)L\mathbf{u}(t)$$

借助如下投影神经网络：

$$\lambda\dot{\mathbf{z}}=-\mathbf{z}+P_{\Omega}(\mathbf{z}-F(\mathbf{z}))$$

其中F(•)为被优化函数的梯度，λ是用于缩放投影神经网络收敛性的参数，且

$$P_{\Omega}(\mathbf{x})=\min_{\mathbf{y}\in\Omega}\|\mathbf{x}-\mathbf{y}\|_2$$

将控制输入带入神经网络便得到了带输入约束的一致性控制律：

$$\lambda\dot{\mathbf{u}}(t)=-\mathbf{u}(t)+P_{\Omega}(\mathbf{u}(t)-\frac{\partial\Phi}{\partial\mathbf{u}}),$$

具体到每个机器人的一致性控制律如下：

$$\lambda\dot{u}_i(t)=-u_i(t)+P_{\Omega}(u_i(t)-\frac{T^5}{10}\sum_{j\in N(i)}(u_i(t)-u_j(t))$$

$$-\frac{T^4}{4}\sum_{j\in N(i)}(v_i(t)-v_j(t))-\frac{T^3}{3}\sum_{j\in N(i)}(x_i(t)-x_j(t)))$$

其中N(i)表示机器人i的邻居节点集合；

所述动力学方程模型中结合Paillier同态加密算法，具体为：

通过显式欧拉法将得到的所述一致性控制律进行离散化，从而得到离散态一致性控制律，离散态一致性控制律如下式；

$$\begin{cases}x_i(k+1)=x_i(k)+\tau v_i(k)\\ v_i(k+1)=v_i(k)+\tau u_i(k)\\ u_i(k+1)=u_i(k)+\frac{\tau}{\lambda}(-u_i(k)+P_{\Omega}(u_i(k)-\frac{T^5}{10}\sum_{j\in N(i)}a_{ij}^k(u_i(k)-u_j(k))\\ -\frac{T^4}{4}\sum_{j\in N(i)}a_{ij}^k(v_i(k)-v_j(k))-\frac{T^3}{3}\sum_{j\in N(i)}a_{ij}^k(x_i(k)-x_j(k)))),\end{cases}$$

其中，k是迭代次数，τ是步长，a_{ij}^k是机器人i和机器人j第k次迭代时的耦合权值，N(i)指机器人i的邻居节点集合；

初始化：每个机器人i初始化相同的系统参数τ，λ，T，并利用Paillier加密算法生成一

个它的公钥pk_i和相应的私钥sk_i,广播公钥到其邻居节点集合N(i),同时保持私钥私有;

迭代:在第k次迭代中,每个机器人i首先使用其公钥pk_i加密状态值:

$x_i(k)\rightarrow\varepsilon_i(x_i(k))$

$v_i(k)\rightarrow\varepsilon_i(v_i(k))$

$u_i(k)\rightarrow\varepsilon_i(u_i(k))$,

然后发送$\varepsilon_i(x_i(k))$,$\varepsilon_i(v_i(k))$,$\varepsilon_i(u_i(k))$到每个邻居机器人j∈N(i);

每个邻居j∈N(i)使用机器人i的公钥pk_i加密$-x_j(k)$:

$-x_j(k)\rightarrow\varepsilon_i(-x_j(k))$

机器人i生成随机数a_i^k,每个邻居j∈N(i)生成随机数a_j^k;

基于Paillier加密算法的加法同态性质,每个邻居j∈N(i)按下式计算加密后的状态差:

$\varepsilon_i(x_i(k))\cdot\varepsilon_i(-x_j(k))=\varepsilon_i(x_i(k)-x_j(k))$,

$$\varepsilon_i(x_i(k)-x_j(k))\rightarrow\varepsilon_i(x_i(k)-x_j(k))^{a_j^k}=\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$$

然后发送以上状态差$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$至机器人i;

机器人i使用私钥sk_i解密收到的状态差值密文,从而得到用于更新自身状态值的状态差值$a_{ij}^k(x_i(k)-x_j(k))$:

$$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))\rightarrow a_j^k(x_i(k)-x_j(k)),$$

$$a_j^k(x_i(k)-x_j(k))\times a_i^k=a_{ij}^k(x_i(k)-x_j(k))$$;

同理可获得$v_i(k)$,$u_i(k)$。

2.一种带隐私保护的一致性最优控制的机器人系统,其特征在于,所述机器人系统的每个机器人均设有:

第一处理单元,其用于建立所述机器人系统中所有机器人在运动时的动力学方程模型;

第二处理单元,其用于在所述动力学方程模型中结合带输入约束的分布式一致性控制律,以获得所有机器人的控制输入;

第三处理单元,其用于在所述动力学方程模型中结合Paillier同态加密算法;以及,

输出单元,其用于将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上,进而使得所有机器人保持运动时位置和速度上保持一致;

所述动力学方程模型具体为:

设无关质量因素的机器人在一维直线上运动,且每个机器人与系统中的部分或全部机器人通信,利用机器人的位置,速度,控制输入和控制输出建立机器人的双积分器动力学方程,具体的,

设机器人具有如下双积分器动力学方程:

$$\begin{cases}\dot{\mathbf{x}}=\mathbf{v}\\ \dot{\mathbf{v}}=\mathbf{u}\\ \mathbf{y}=\mathbf{x}\end{cases}$$

其中x＝[x_1,x_2…x_n]^T,v＝[v_1,v_2…v_n]^{T}表示各个机器人们的状态向量,u＝[u_1,u_2…u_n]^T,y＝[y_1,y_2…y_n]^{T}分别表示各个机器人的状态向量输入向量和输出向量,对于第i个机器人x_i,v_i,u_i,y_i分别代表其位置,速度,控制输入和控制输出;

设无关质量因素的机器人在二维平面上和三维空间上运动,且每个机器人与系统中的部分或全部机器人通信,利用机器人的位置,速度,控制输入和控制输出建立机器人的双积分器动力学方程,具体的,先分别计算各二维、三维坐标轴方向对应的控制输入值,然后矢量合成为一个方向的控制输入值,最终让每个机器人的位置达到一致;

所述带输入约束的分布式一致性控制律,具体为:

借助如下积分型性能指标

$$J_{\mathrm{d}}(t)=\int_0^T\mathbf{y}^{\mathrm{T}}(t+\tau)L\mathbf{y}(t+\tau)\mathrm{d}\tau$$

其中L是多智能体系统对应拓扑图的拉普拉斯矩阵,T称为预测间隔,得到如下优化问题

min $J_d(t)$

$$\text{subject to }\ \dot{\mathbf{x}}=\mathbf{v}$$

$$\dot{\mathbf{v}}=\mathbf{u}$$

y＝x

u∈Ω

其中Ω是一个关于输入的闭合凸集合,约定了输入的上下界,通过泰勒展开

$$\mathbf{y}(t+\tau)\approx\mathbf{y}(t)+\tau\dot{\mathbf{y}}(t)+\frac{\tau^2}{2}\ddot{\mathbf{y}}(t)$$

$$=\mathbf{x}(t)+\tau\mathbf{v}(t)+\frac{\tau^2}{2}\mathbf{u}(t).$$

代入上述优化问题,经过简化及省略与输入u无关的部分,得到剩余

$$\Phi=\frac{T^5}{20}\mathbf{u}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^4}{4}\mathbf{v}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^3}{3}\mathbf{x}^{\mathrm{T}}(t)L\mathbf{u}(t)$$

借助如下投影神经网络:

$$\lambda\dot{\mathbf{z}}=-\mathbf{z}+P_{\Omega}(\mathbf{z}-F(\mathbf{z}))$$

其中F(•)为被优化函数的梯度,λ是用于缩放投影神经网络收敛性的参数,且

$$P_{\Omega}(\mathbf{x})=\min_{\mathbf{y}\in\Omega}\|\mathbf{x}-\mathbf{y}\|_2$$

将控制输入带入神经网络便得到了带输入约束的一致性控制律:

$$\lambda\dot{\mathbf{u}}(t)=-\mathbf{u}(t)+P_{\Omega}(\mathbf{u}(t)-\frac{\partial\Phi}{\partial\mathbf{u}}),$$

具体到每个机器人的一致性控制律如下：

$$\lambda\dot{u}_i(t)=-u_i(t)+P_{\Omega}(u_i(t)-\frac{T^5}{10}\sum_{j\in N(i)}(u_i(t)-u_j(t))$$

$$-\frac{T^4}{4}\sum_{j\in N(i)}(v_i(t)-v_j(t))-\frac{T^3}{3}\sum_{j\in N(i)}(x_i(t)-x_j(t)))$$

其中N(i)表示机器人i的邻居节点集合；

所述动力学方程模型中结合Paillier同态加密算法，具体为：

通过显式欧拉法将得到的所述一致性控制律进行离散化，从而得到离散态一致性控制律，离散态一致性控制律如下式；

$$\begin{cases}x_i(k+1)=x_i(k)+\tau v_i(k)\\ v_i(k+1)=v_i(k)+\tau u_i(k)\\ u_i(k+1)=u_i(k)+\frac{\tau}{\lambda}(-u_i(k)+P_{\Omega}(u_i(k)-\frac{T^5}{10}\sum_{j\in N(i)}a_{ij}^k(u_i(k)-u_j(k))\\ -\frac{T^4}{4}\sum_{j\in N(i)}a_{ij}^k(v_i(k)-v_j(k))-\frac{T^3}{3}\sum_{j\in N(i)}a_{ij}^k(x_i(k)-x_j(k)))),\end{cases}$$

其中，k是迭代次数，τ是步长，a_{ij}^k是机器人i和机器人j第k次迭代时的耦合权值，N(i)指机器人i的邻居节点集合；

初始化：每个机器人i初始化相同的系统参数τ，λ，T，并利用Paillier加密算法生成一个它的公钥pk_i和相应的私钥sk_i，广播公钥到其邻居节点集合N(i)，同时保持私钥私有；

迭代：在第k次迭代中，每个机器人i首先使用其公钥pk_i加密状态值：

$x_i(k)\rightarrow\varepsilon_i(x_i(k))$

$v_i(k)\rightarrow\varepsilon_i(v_i(k))$

$u_i(k)\rightarrow\varepsilon_i(u_i(k))$，

然后发送$\varepsilon_i(x_i(k))$，$\varepsilon_i(v_i(k))$，$\varepsilon_i(u_i(k))$到每个邻居机器人j∈N(i)；

每个邻居j∈N(i)使用机器人i的公钥pk_i加密$-x_j(k)$：

$-x_j(k)\rightarrow\varepsilon_i(-x_j(k))$

机器人i生成随机数a_i^k，每个邻居j∈N(i)生成随机数a_j^k；

基于Paillier加密算法的加法同态性质，每个邻居j∈N(i)按下式计算加密后的状态差：

$\varepsilon_i(x_i(k))\cdot\varepsilon_i(-x_j(k))=\varepsilon_i(x_i(k)-x_j(k))$，

$$\varepsilon_i(x_i(k)-x_j(k))\rightarrow\varepsilon_i(x_i(k)-x_j(k))^{a_j^k}=\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$$

然后发送以上状态差$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$至机器人i；

机器人i使用私钥sk_i解密收到的状态差值密文，从而得到用于更新自身状态值的状态差值$a_{ij}^k(x_i(k)-x_j(k))$：

$$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))\rightarrow a_j^k(x_i(k)-x_j(k)),$$

$$a_j^k(x_i(k)-x_j(k))\times a_i^k=a_{ij}^k(x_i(k)-x_j(k))\ ;$$

同理可获得$v_i(k)$，$u_i(k)$。

3.一种电子设备，其特征在于，所述电子设备包括处理器和存储器，所述存储器中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器加载并执行，以实现如权利要求1所述的带隐私保护的一致性最优控制方法。

4.一种计算机可读存储介质，其特征在于，所述存储介质中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由处理器加载并执行以实现权利要求1所述的带隐私保护的一致性最优控制方法。

带隐私保护的一致性最优控制方法、系统、设备和介质

技术领域

[0001] 本发明涉及控制领域和机器人领域，具体涉及一种带隐私保护的一致性最优控制方法、系统、设备和介质。

背景技术

[0002] 多智能体系统的一致性控制作为协同控制和分布式计算一个重要的分支，因其鲁棒性和可伸缩性而广泛应用在各个领域，如编队控制，智能机器人系统，传感器网络和智能电网。所谓一致性，是指多智能体系统的个体基于邻居信息调节更新自己的行为，最终使得每个个体就某个状态达成一致，解决一致性问题的关键是为系统中的个体设计算法或控制律，一般而言是分布式算法或控制律，而传统的一致性算法往往都需要个体之间交换状态值以更新状态值，但如果个体状态值或者初始状态值是私有敏感数据，则存在隐私泄露的担忧。

发明内容

[0003] 针对现有技术中的不足，本发明提供一种带隐私保护的一致性最优控制方法、系统、设备和介质，使得所有机器人最终在位置和速度上保持一致，同时避免泄露私有信息。

[0004] 为实现上述目的，本发明可以采用如下技术方案：

[0005] 一种带隐私保护的一致性最优控制方法，应用于机器人系统，其包括如下步骤：

[0006] 建立所述机器人系统中所有机器人在运动时的动力学方程模型；

[0007] 在所述动力学方程模型中结合带输入约束的分布式一致性控制律，以获得所有机器人的控制输入；

[0008] 在所述动力学方程模型中结合Paillier同态加密算法；

[0009] 将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上，进而使得所有机器人保持运动时位置和速度上保持一致。

[0010] 如上所述的带隐私保护的一致性最优控制方法，进一步的，所述动力学方程模型具体为：

[0011] 设无关质量因素的机器人在一维直线上运动，且每个机器人与系统中的部分或全部机器人通信，利用机器人的位置，速度，控制输入和控制输出建立机器人的双积分器动力学方程，具体的，

[0012] 设机器人具有如下双积分器动力学方程：$$\begin{cases}\dot{\mathbf{x}}=\mathbf{v}\\ \dot{\mathbf{v}}=\mathbf{u}\\ \mathbf{y}=\mathbf{x}\end{cases}$$

[0013] 其中$\mathrm{x}=[\mathrm{x}_1,\mathrm{x}_2\cdots\mathrm{x}_n]^{\mathrm{T}},\mathrm{v}=[\mathrm{v}_1,\mathrm{v}_2\cdots\mathrm{v}_n]^{\mathrm{T}},\mathrm{u}=[\mathrm{u}_1,\mathrm{u}_2\cdots\mathrm{u}_n]^{\mathrm{T}},\mathrm{y}=[\mathrm{y}_1,\mathrm{y}_2\cdots\mathrm{y}_n]^{\mathrm{T}}$分别表示机器人们的状态向量，输入向量和输出向量，对于第i个机器人x_i,v_i,u_i,y_i可以分别代表其位

置，速度，控制输入和控制输出。

[0014] 如上所述的带隐私保护的一致性最优控制方法，进一步的，设无关质量因素的机器人在二维平面上和三维空间上运动，且每个机器人与系统中的部分或全部机器人通信，利用机器人的位置，速度，控制输入和控制输出建立机器人的双积分器动力学方程，具体的，先分别计算各二维、三维坐标轴方向对应的控制输入值，然后矢量合成为一个方向的控制输入值，最终让每个机器人的位置达到一致。

[0015] 如上所述的带隐私保护的一致性最优控制方法，进一步的，所述带输入约束的分布式一致性控制律，具体为：

[0016] 借助如下积分型性能指标 $J_{\mathrm{d}}(t)=\int_0^T \mathbf{y}^{\mathrm{T}}(t+\tau)L\mathbf{y}(t+\tau)\mathrm{d}\tau$

[0017] 其中L是多智能体系统对应拓扑图的拉普拉斯矩阵，T称为预测间隔，得到如下优化问题

[0018]
$$\begin{aligned}\min\ & J_{\mathrm{d}}(t)\\ \text{subject to}\ & \dot{\mathbf{x}}=\mathbf{v}\\ & \dot{\mathbf{v}}=\mathbf{u}\\ & \mathbf{y}=\mathbf{x}\\ & \mathbf{u}\in\Omega\end{aligned}$$

[0019] 其中Ω是一个关于输入的闭合凸集合，约定了输入的上下界。通过泰勒展开

[0020]
$$\begin{aligned}\mathbf{y}(t+\tau)&\approx\mathbf{y}(t)+\tau\dot{\mathbf{y}}(t)+\frac{\tau^2}{2}\ddot{\mathbf{y}}(t)\\ &=\mathbf{x}(t)+\tau\mathbf{v}(t)+\frac{\tau^2}{2}\mathbf{u}(t).\end{aligned}$$

[0021] 代入上述优化问题，经过简化及省略与输入u无关的部分，得到剩余

[0022] $$\Phi=\frac{T^5}{20}\mathbf{u}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^4}{4}\mathbf{v}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^3}{3}\mathbf{x}^{\mathrm{T}}(t)L\mathbf{u}(t)$$

[0023] 借助如下投影神经网络：

[0024] $$\lambda\dot{\mathbf{z}}=-\mathbf{z}+P_{\Omega}(\mathbf{z}-F(\mathbf{z}))$$

[0025] 其中$F(\bullet)$为被优化函数的梯度，λ是用于缩放投影神经网络收敛性的参数，且

[0026] $$P_{\Omega}(\mathbf{x})=\min_{\mathbf{y}\in\Omega}\|\mathbf{x}-\mathbf{y}\|_2$$

[0027] 将控制输入带入神经网络便得到了带输入约束的一致性控制律：

[0028] $$\lambda\dot{\mathbf{u}}(t)=-\mathbf{u}(t)+P_{\Omega}(\mathbf{u}(t)-\frac{\partial\Phi}{\partial\mathbf{u}})。$$

[0029] 如上所述的带隐私保护的一致性最优控制方法，进一步的，具体到每个机器人的一致性控制律如下：

[0030]
$$\lambda \dot{u}_i(t) = -u_i(t) + P_\Omega(u_i(t) - \frac{T^5}{10}\sum_{j\in N(i)}(u_i(t)-u_j(t)) - \frac{T^4}{4}\sum_{j\in N(i)}(v_i(t)-v_j(t)) - \frac{T^3}{3}\sum_{j\in N(i)}(x_i(t)-x_j(t)))$$

[0031] 其中 $N(i)$ 表示机器人 i 的邻居节点集合。

[0032] 如上所述的带隐私保护的一致性最优控制方法，进一步的，所述动力学方程模型中结合Paillier同态加密算法，具体为：

[0033] 通过显式欧拉法将得到的所述一致性控制律进行离散化，从而得到离散态一致性控制律，离散态一致性控制律如下式；

[0034]
$$\begin{cases} x_i(k+1) = x_i(k) + \tau v_i(k) \\ v_i(k+1) = v_i(k) + \tau u_i(k) \\ u_i(k+1) = u_i(k) + \frac{\tau}{\lambda}(-u_i(k) + P_\Omega(u_i(k) - \frac{T^5}{10}\sum_{j\in N(i)} a_{ij}^k(u_i(k)-u_j(k)), \\ -\frac{T^4}{4}\sum_{j\in N(i)} a_{ij}^k(v_i(k)-v_j(k)) - \frac{T^3}{3}\sum_{j\in N(i)} a_{ij}^k(x_i(k)-x_j(k)))) \end{cases}$$

[0035] 其中，k 是迭代次数，τ 是步长，a_{ij}^k 是机器人 i 和机器人 j 第 k 次迭代时的耦合权值，$N(i)$ 指机器人 i 相互通信的邻居节点集合；

[0036] 初始化：每个机器人 i 初始化相同的系统参数 τ, λ, T，并利用Paillier加密算法生成一个它的公钥 pk_i 和相应的私钥 sk_i，广播公钥到其邻居们 $N(i)$，同时保持私钥私有；

[0037] 迭代：在第k次迭代中，每个机器人 i 首先使用其公钥 pk_i 加密状态值：

[0038]
$$x_i(k) \to \varepsilon_i(x_i(k)), \quad v_i(k) \to \varepsilon_i(v_i(k)), \quad u_i(k) \to \varepsilon_i(u_i(k))$$

[0039] 然后发送 $\varepsilon_i(x_i(k)), \varepsilon_i(v_i(k)), \varepsilon_i(u_i(k))$ 到每个邻居机器人 $j \in N(i)$；

[0040] 每个邻居 $j \in N(i)$ 使用机器人 i 的公钥 pk_i 加密 $-x_j(k)$：

[0041] $-x_j(k) \to \varepsilon_i(-x_j(k))$

[0042] 机器人 i 生成随机数 a_i^k，每个邻居 $j \in N(i)$ 生成随机数 a_j^k；

[0043] 基于Paillier加密算法的加法同态性质，每个邻居 $j \in N(i)$ 按下式计算加密后

的状态差：

[0044] $\varepsilon_i(x_i(k))\cdot\varepsilon_i(-x_j(k))=\varepsilon_i(x_i(k)-x_j(k))$，

[0045] $\varepsilon_i(x_i(k)-x_j(k))\rightarrow\varepsilon_i(x_i(k)-x_j(k))^{a_j^k}=\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$

[0046] 然后发送以上状态差$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$至机器人$i$；

[0047] 机器人i使用私钥sk_i解密收到的状态差值密文，从而得到用于更新自身状态值的状态差值$a_{ij}^k(x_i(k)-x_j(k))$：

[0048] $\varepsilon_i(a_j^k(x_i(k)-x_j(k)))\rightarrow a_j^k(x_i(k)-x_j(k))$，

[0049] $a_j^k(x_i(k)-x_j(k))\times a_i^k=a_{ij}^k(x_i(k)-x_j(k))$；

[0050] 同理可获得$v_i(k),u_i(k)$。

[0051] 一种带隐私保护的一致性最优控制的机器人系统，所述机器人系统的每个机器人均设有：

[0052] 第一处理单元，其用于建立所述机器人系统中所有机器人在运动时的动力学方程模型；

[0053] 第二处理单元，其用于在所述动力学方程模型中结合带输入约束的分布式一致性控制律，以获得所有机器人的控制输入；

[0054] 第三处理单元，其用于在所述动力学方程模型中结合Paillier同态加密算法；以及，输出单元，其用于将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上，进而使得所有机器人保持运动时位置和速度上保持一致。

[0055] 一种电子设备，所述电子设备包括处理器和存储器，所述存储器中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器加载并执行，以实现如上所述的带隐私保护的一致性最优控制方法。

[0056] 一种计算机可读存储介质，所述存储介质中存储有至少一条指令、至少一段程序、代码集或指令集，所述至少一条指令、所述至少一段程序、所述代码集或指令集由处理器加载并执行以实现如上所述的带隐私保护的一致性最优控制方法。

[0057] 本发明与现有技术相比，其有益效果在于：本发明在一致性最优控制方法的基础上，嵌入隐私保护机制，所有机器人遵守隐私保护机制中的流程，在每次迭代中与其邻居交换加密后的状态信息，获得用于更新自身状态信息的状态差值，将状态差值代入离散化后的一致性控制律中便得到了控制输入，然后将得到的控制输入施加到机器人上，如此循环反复，最终令所有机器人在位置，速度上保持一致，同时保持私有信息不泄露。

附图说明

[0058] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例中所需要使用的附图进行简单的介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本

领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0059] 图1为本发明实施例的带隐私保护的一致性最优控制方法的流程图；

[0060] 图2为本发明实施例的带隐私保护的一致性最优控制的机器人系统的结构示意图；

[0061] 图3为本发明实施例的电子设备的结构示意图。

具体实施方式

[0062] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整的描述，显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0063] 实施例：

[0064] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或描述的那些以外的顺序实施。此外，本发明实施例的术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0065] 下文中所用的词语“示例性”的意思为“用作例子、实施例或说明性”。作为“示例性”所说明的任何实施例不必解释为优于或好于其它实施例。

[0066] 为更好地理解本发明实施例提供的技术方案，下面对本发明实施例提供的技术方案的技术背景做一些简单介绍，以便更好理解本发明的技术构思。

[0067] 传统的一致性算法往往都需要个体之间交换状态值以更新状态值，但如果个体状态值或者初始状态值是私有敏感数据，则存在隐私泄露的担忧。

[0068] 基于此，本发明在一致性最优控制方法的基础上，嵌入隐私保护机制，所有机器人遵守隐私保护机制中的流程，在每次迭代中与其邻居交换加密后的状态信息，获得用于更新自身状态信息的状态差值，将状态差值代入离散化后的一致性控制律中便得到了控制输入，然后将得到的控制输入施加到机器人上，如此循环反复，最终令所有机器人在位置，速度上保持一致，同时保持私有信息不泄露。

[0069] 参见图1，一种带隐私保护的一致性最优控制方法，其可以包括如下步骤：

[0070] 步骤1：建立机器人运动时的动力学方程模型；

[0071] 步骤2：基于步骤1的模型，设计带输入约束的分布式一致性控制律来求得所有机器人的控制输入；

[0072] 步骤3：基于步骤2中的一致性控制律，结合Paillier同态加密算法，设计带隐私保护的机器人系统的一致性最优控制方法；

[0073] 步骤4：在机器人上应用步骤3中的一致性最优控制方法的基础上，嵌入隐私保护机制，将得到的控制输入施加到机器人上，令所有机器人最终在位置，速度上保持一致。

[0074] 作为一种可选的实施方式，在某些实施例中，所述步骤1中建立机器人运动时的动力学方程模型，在不考虑机器人实际对应的质量大小前提下，考虑机器人在一维直线上运动，且一个机器人与系统中的部分或全部机器人通信，通信拓扑图可以用一个无向连通图来表示，设机器人具有如下双积分器动力学方程：

[0075] $$\begin{cases}\dot{\mathbf{x}}=\mathbf{v}\\ \dot{\mathbf{v}}=\mathbf{u}\\ \mathbf{y}=\mathbf{x}\end{cases}$$

[0076] 其中 $\mathbf{x}=[x_1,x_2\cdots x_n]^{\mathrm{T}},\mathbf{v}=[v_1,v_2\cdots v_n]^{\mathrm{T}},\mathbf{u}=[u_1,u_2\cdots u_n]^{\mathrm{T}},\mathbf{y}=[y_1,y_2\cdots y_n]^{\mathrm{T}}$ 分别表示机器人们的状态向量，输入向量和输出向量，对于第 i 个机器人 x_i,v_i,u_i,y_i 可以分别代表其位置，速度，控制输入和输出。需要设计一个一致性控制方法，来求得所有机器人的控制输入，并使得最终每个机器人的位置达到一致，即对任意的两个机器人 i,j 有 $x_i=x_j$。

[0077] 进一步的，考虑二维平面上和三维空间中的机器人运动，可以分别计算各坐标轴方向对应的控制输入值，然后合成为一个方向的控制输入值，最终让每个机器人的位置达到一致。

[0078] 作为一种可选的实施方式，在某些实施例中，所述步骤2中设计带输入约束的分布式一致性控制律来求得所有机器人的控制输入，一致性控制律具体如下：

[0079] 借助如下积分型性能指标

[0080] $$J_{\mathrm{d}}(t)=\int_0^T\mathbf{y}^{\mathrm{T}}(t+\tau)L\mathbf{y}(t+\tau)\mathrm{d}\tau$$

[0081] 其中 L 是多智能体系统对应拓扑图的拉普拉斯矩阵，T 称为预测间隔，得到如下优化问题

[0082] $$\begin{aligned}\min\ & J_{\mathrm{d}}(t)\\ \text{subject to}\ & \dot{\mathbf{x}}=\mathbf{v}\\ & \dot{\mathbf{v}}=\mathbf{u}\\ & \mathbf{y}=\mathbf{x}\\ & \mathbf{u}\in\Omega\end{aligned}$$

[0083] 其中 Ω 是一个关于输入的闭合凸集合，约定了输入的上下界。通过泰勒展开

[0084] $$\begin{aligned}\mathbf{y}(t+\tau)&\approx\mathbf{y}(t)+\tau\dot{\mathbf{y}}(t)+\frac{\tau^2}{2}\ddot{\mathbf{y}}(t)\\ &=\mathbf{x}(t)+\tau\mathbf{v}(t)+\frac{\tau^2}{2}\mathbf{u}(t).\end{aligned}$$

[0085] 代入上述优化问题，经过简化及省略与输入 u 无关的部分，得到剩余

[0086] $$\Phi=\frac{T^5}{20}\mathbf{u}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^4}{4}\mathbf{v}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^3}{3}\mathbf{x}^{\mathrm{T}}(t)L\mathbf{u}(t)$$

[0087] 借助如下投影神经网络：

[0088] $$\lambda\dot{\mathbf{z}}=-\mathbf{z}+P_{\Omega}(\mathbf{z}-F(\mathbf{z}))$$

[0089] 其中$F(\bullet)$为被优化函数的梯度，λ是用于缩放投影神经网络收敛性的参数，且

[0090] $$P_{\Omega}(\mathbf{x})=\min_{\mathbf{y}\in\Omega}\|\mathbf{x}-\mathbf{y}\|_2$$

[0091] 将控制输入带入神经网络便得到了带输入约束的一致性控制律：

[0092] $$\lambda\dot{\mathbf{u}}(t)=-\mathbf{u}(t)+P_{\Omega}(\mathbf{u}(t)-\frac{\partial\Phi}{\partial\mathbf{u}})$$

[0093] 更进一步，具体到每个机器人的一致性控制律如下

[0094] $$\begin{aligned}\lambda\dot{u}_i(t)=&-u_i(t)+P_{\Omega}(u_i(t)-\frac{T^5}{10}\sum_{j\in N(i)}(u_i(t)-u_j(t))\\&-\frac{T^4}{4}\sum_{j\in N(i)}(v_i(t)-v_j(t))-\frac{T^3}{3}\sum_{j\in N(i)}(x_i(t)-x_j(t)))\end{aligned}\quad(1)$$

[0095] 其中$N(i)$表示机器人i的邻居节点集合。

[0096] 作为一种可选的实施方式，在某些实施例中，所述步骤3基于步骤2中的一致性控制律，通过显式欧拉法将得到的一致性控制律(1)进行离散化得到

[0097] $$\begin{cases}x_i(k+1)=x_i(k)+\tau v_i(k)\\v_i(k+1)=v_i(k)+\tau u_i(k)\\u_i(k+1)=u_i(k)+\frac{\tau}{\lambda}(-u_i(k)+P_{\Omega}(u_i(k)-\frac{T^5}{10}\sum_{j\in N(i)}a_{ij}^k(u_i(k)-u_j(k))\\-\frac{T^4}{4}\sum_{j\in N(i)}a_{ij}^k(v_i(k)-v_j(k))-\frac{T^3}{3}\sum_{j\in N(i)}a_{ij}^k(x_i(k)-x_j(k)))),\end{cases}\quad(2)$$

[0098] 其中，k是迭代次数，τ是步长，a_{ij}^k是机器人i和机器人j第k次迭代时的耦合权值，$N(i)$指机器人i相互通信的邻居节点集合。从离散态一致性控制律(2)中可见，机器人i更新控制输入时需要和其邻居节点交换状态值x_i,v_i,u_i，这引起隐私泄露的担忧，结合Paillier同态加密算法，设计带隐私保护的机器人系统的一致性最优控制方法，以一次状态交换过程为例，隐私保护方案具体如下：

[0099] 步骤301、初始化：每个机器人i初始化相同的系统参数τ,λ,T，并利用Paillier加密算法生成一个它的公钥pk_i和相应的私钥sk_i，广播公钥到其邻居们$N(i)$，同时保持私钥私有。

[0100] 步骤302、迭代：

[0101] (1).在第k次迭代中，每个机器人i首先使用其公钥pk_i加密状态值：

[0102] $$x_i(k)\to\varepsilon_i(x_i(k))$$
$$v_i(k)\to\varepsilon_i(v_i(k)),$$
$$u_i(k)\to\varepsilon_i(u_i(k))$$

[0103] 然后发送$\varepsilon_i(x_i(k)),\varepsilon_i(v_i(k)),\varepsilon_i(u_i(k))$到每个邻居机器人$j\in N(i)$。(由于$x_i(k),v_i(k),u_i(k)$本质都是表示机器人的状态值,且都应该保证不泄露,故接下来仅具体表明对$x_i(k)$的操作,但这些操作步骤应同时对$v_i(k),u_i(k)$实施。)

[0104] (2).每个邻居$j\in N(i)$使用机器人i的公钥pk_i加密$-x_j(k)$:

[0105] $$-x_j(k)\to\varepsilon_i(-x_j(k))$$

[0106] (3).机器人i生成随机数a_i^k,每个邻居$j\in N(i)$生成随机数a_j^k。

[0107] (4).基于Paillier加密算法的加法同态性质,每个邻居$j\in N(i)$按下式计算加密后的状态差:

[0108] $$\varepsilon_i(x_i(k))\cdot\varepsilon_i(-x_j(k))=\varepsilon_i(x_i(k)-x_j(k)),$$
$$\varepsilon_i(x_i(k)-x_j(k))\to\varepsilon_i(x_i(k)-x_j(k))^{a_j^k}=\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$$

[0109] 然后发送以上状态差$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))$至机器人$i$。

[0110] (5).机器人i使用私钥sk_i解密收到的状态差值密文,便得到了用于更新自身状态值的状态差值$a_{ij}^k(x_i(k)-x_j(k))$($v_i(k),u_i(k)$同理):

[0111] $$\varepsilon_i(a_j^k(x_i(k)-x_j(k)))\to a_j^k(x_i(k)-x_j(k)),$$

[0112] $$a_j^k(x_i(k)-x_j(k))\times a_i^k=a_{ij}^k(x_i(k)-x_j(k))。$$

[0113] 作为一种可选的实施方式,在某些实施例中,所述步骤4在机器人上应用步骤3中的带隐私保护的一致性最优控制方法,将得到的控制输入施加到机器人上,令所有机器人最终在位置,速度上保持一致,同时保证私有信息不泄露。

[0114] 参见图2,基于同一发明构思,本发明实施例还提供一种带隐私保护的一致性最优控制的机器人系统,所述机器人系统的每个机器人均设有:第一处理单元、第二处理单元、第三处理单元和输出单元,其中,第一处理单元用于建立所述机器人系统中所有机器人在运动时的动力学方程模型;第二处理单元用于在所述动力学方程模型中结合带输入约束的分布式一致性控制律,以获得所有机器人的控制输入;第三处理单元用于在所述动力学方程模型中结合Paillier同态加密算法;输出单元用于将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上,进而使得所有机器人保持运动时位置和速度上保持一致。

[0115] 作为一种可选的实施方式，第一处理单元用于处理以下过程数据：建立机器人运动时的动力学方程模型，在不考虑机器人实际对应的质量大小前提下，考虑机器人在一维直线上运动，且一个机器人与系统中的部分或全部机器人通信，通信拓扑图可以用一个无向连通图来表示，设机器人具有如下双积分器动力学方程：

[0116] $$\begin{cases}\dot{\mathbf{x}}=\mathbf{v}\\ \dot{\mathbf{v}}=\mathbf{u}\\ \mathbf{y}=\mathbf{x}\end{cases}$$

[0117] 其中 $\mathbf{x}=[x_1,x_2\cdots x_n]^{\mathrm{T}},\mathbf{v}=[v_1,v_2\cdots v_n]^{\mathrm{T}},\mathbf{u}=[u_1,u_2\cdots u_n]^{\mathrm{T}},\mathbf{y}=[y_1,y_2\cdots y_n]^{\mathrm{T}}$ 分别表示机器人们的状态向量，输入向量和输出向量，对于第 i 个机器人 x_i,v_i,u_i,y_i 可以分别代表其位置，速度，控制输入和输出。需要设计一个一致性控制方法，来求得所有机器人的控制输入，并使得最终每个机器人的位置达到一致，即对任意的两个机器人 i,j 有 $x_i=x_j$。

[0118] 进一步的，考虑二维平面上和三维空间中的机器人运动，可以分别计算各坐标轴方向对应的控制输入值，然后合成为一个方向的控制输入值，最终让每个机器人的位置达到一致。

[0119] 作为一种可选的实施方式，第二处理单元用于处理以下过程数据：设计带输入约束的分布式一致性控制律来求得所有机器人的控制输入，一致性控制律具体如下：

[0120] 借助如下积分型性能指标

[0121] $$J_{\mathrm{d}}(t)=\int_0^T\mathbf{y}^{\mathrm{T}}(t+\tau)L\mathbf{y}(t+\tau)\mathrm{d}\tau$$

[0122] 其中 L 是多智能体系统对应拓扑图的拉普拉斯矩阵，T 称为预测间隔，得到如下优化问题

[0123] $$\begin{aligned}\min\ & J_{\mathrm{d}}(t)\\ \text{subject to}\ & \dot{\mathbf{x}}=\mathbf{v}\\ & \dot{\mathbf{v}}=\mathbf{u}\\ & \mathbf{y}=\mathbf{x}\\ & \mathbf{u}\in\Omega\end{aligned}$$

[0124] 其中 Ω 是一个关于输入的闭合凸集合，约定了输入的上下界。通过泰勒展开

[0125] $$\begin{aligned}\mathbf{y}(t+\tau)&\approx\mathbf{y}(t)+\tau\dot{\mathbf{y}}(t)+\frac{\tau^2}{2}\ddot{\mathbf{y}}(t)\\ &=\mathbf{x}(t)+\tau\mathbf{v}(t)+\frac{\tau^2}{2}\mathbf{u}(t).\end{aligned}$$

[0126] 代入上述优化问题，经过简化及省略与输入 u 无关的部分，得到剩余

[0127] $$\Phi=\frac{T^5}{20}\mathbf{u}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^4}{4}\mathbf{v}^{\mathrm{T}}(t)L\mathbf{u}(t)+\frac{T^3}{3}\mathbf{x}^{\mathrm{T}}(t)L\mathbf{u}(t)$$

[0128] 借助如下投影神经网络：

[0129] $$\lambda\dot{\mathbf{z}}=-\mathbf{z}+P_{\Omega}(\mathbf{z}-F(\mathbf{z}))$$

[0130] 其中$F(\bullet)$为被优化函数的梯度，λ是用于缩放投影神经网络收敛性的参数，且

[0131] $$P_{\Omega}(\mathbf{x})=\min_{\mathbf{y}\in\Omega}\|\mathbf{x}-\mathbf{y}\|_2$$

[0132] 将控制输入带入神经网络便得到了带输入约束的一致性控制律：

[0133] $$\lambda\dot{\mathbf{u}}(t)=-\mathbf{u}(t)+P_{\Omega}(\mathbf{u}(t)-\frac{\partial\Phi}{\partial\mathbf{u}})$$

[0134] 更进一步，具体到每个机器人的一致性控制律如下

[0135] $$\begin{aligned}\lambda\dot{u}_i(t)=&-u_i(t)+P_{\Omega}(u_i(t)-\frac{T^5}{10}\sum_{j\in N(i)}(u_i(t)-u_j(t))\\&-\frac{T^4}{4}\sum_{j\in N(i)}(v_i(t)-v_j(t))-\frac{T^3}{3}\sum_{j\in N(i)}(x_i(t)-x_j(t)))\end{aligned}\quad(1)$$

[0136] 其中$N(i)$表示机器人i的邻居节点集合。

[0137] 作为一种可选的实施方式，在第三处理单元用于处理以下过程数据：基于第二处理单元的一致性控制律，通过显式欧拉法将得到的一致性控制律(1)进行离散化得到

[0138] $$\begin{cases}x_i(k+1)=x_i(k)+\tau v_i(k)\\v_i(k+1)=v_i(k)+\tau u_i(k)\\u_i(k+1)=u_i(k)+\frac{\tau}{\lambda}(-u_i(k)+P_{\Omega}(u_i(k)-\frac{T^5}{10}\sum_{j\in N(i)}a_{ij}^k(u_i(k)-u_j(k))\\-\frac{T^4}{4}\sum_{j\in N(i)}a_{ij}^k(v_i(k)-v_j(k))-\frac{T^3}{3}\sum_{j\in N(i)}a_{ij}^k(x_i(k)-x_j(k)))),\end{cases}\quad(2)$$

[0139] 其中，k是迭代次数，τ是步长，a_{ij}^k是机器人i和机器人j第k次迭代时的耦合权值，$N(i)$指机器人i相互通信的邻居节点集合。从离散态一致性控制律(2)中可见，机器人i更新控制输入时需要和其邻居节点交换状态值x_i,v_i,u_i，这引起隐私泄露的担忧，结合Paillier同态加密算法，设计带隐私保护的机器人系统的一致性最优控制方法，以一次状态交换过程为例，隐私保护方案具体如下：

[0140] 步骤301、初始化：每个机器人i初始化相同的系统参数τ,λ,T，并利用Paillier加密算法生成一个它的公钥pk_i和相应的私钥sk_i，广播公钥到其邻居们$N(i)$，同时保持私钥私有。

[0141] 步骤302、迭代：

[0142] (1).在第k次迭代中,每个机器人i首先使用其公钥pk_i加密状态值:

$$x_i(k) \to \varepsilon_i(x_i(k))$$

[0143] $$v_i(k) \to \varepsilon_i(v_i(k)),$$

$$u_i(k) \to \varepsilon_i(u_i(k))$$

[0144] 然后发送$\varepsilon_i(x_i(k)),\varepsilon_i(v_i(k)),\varepsilon_i(u_i(k))$到每个邻居机器人$j \in N(i)$。(由于$x_i(k),v_i(k),u_i(k)$本质都是表示机器人的状态值,且都应该保证不泄露,故接下来仅具体表明对$x_i(k)$的操作,但这些操作步骤应同时对$v_i(k),u_i(k)$实施。)

[0145] (2).每个邻居$j \in N(i)$使用机器人i的公钥pk_i加密$-x_j(k)$:

[0146] $$-x_j(k) \to \varepsilon_i(-x_j(k))。$$

[0147] (3).机器人i生成随机数a_i^k,每个邻居$j \in N(i)$生成随机数a_j^k。

[0148] (4).基于Paillier加密算法的加法同态性质,每个邻居$j \in N(i)$按下式计算加密后的状态差:

[0149] $$\varepsilon_i(x_i(k)) \cdot \varepsilon_i(-x_j(k)) = \varepsilon_i(x_i(k) - x_j(k)),$$

[0150] $$\varepsilon_i(x_i(k) - x_j(k)) \to \varepsilon_i(x_i(k) - x_j(k))^{a_j^k} = \varepsilon_i(a_j^k(x_i(k) - x_j(k)))$$

[0151] 然后发送以上状态差$\varepsilon_i(a_j^k(x_i(k) - x_j(k)))$至机器人$i$。

[0152] (5).机器人i使用私钥sk_i解密收到的状态差值密文,便得到了用于更新自身状态值的状态差值$a_{ij}^k(x_i(k) - x_j(k))$($v_i(k),u_i(k)$同理):

[0153] $$\varepsilon_i(a_j^k(x_i(k) - x_j(k))) \to a_j^k(x_i(k) - x_j(k)),$$

[0154] $$a_j^k(x_i(k) - x_j(k)) \times a_i^k = a_{ij}^k(x_i(k) - x_j(k))。$$

[0155] 作为一种可选的实施方式,输出单元用于处理以下过程数据:输出单元在机器人上应用第三处理单元中的带隐私保护的一致性最优控制方法,将得到的控制输入施加到机器人上,令所有机器人最终在位置,速度上保持一致,同时保证私有信息不泄露。

[0156] 由于该系统是本发明实施例的带隐私保护的一致性最优控制方法对应的系统,并且该系统解决问题的原理与该方法相似,因此该系统的实施可以参见上述方法实施例的实施过程,重复之处不再赘述。

[0157] 参见图3,基于同一发明构思,本发明实施例还提供一种电子设备,所述电子设备包括处理器和存储器,所述存储器中存储有至少一条指令、至少一段程序、代码集或指令

集,所述至少一条指令、所述至少一段程序、所述代码集或指令集由所述处理器加载并执行,以实现如上所述的带隐私保护的一致性最优控制方法。

[0158] 可以理解的是,存储器可以包括随机存储器(Random Access Memory,RAM),也可以包括只读存储器(Read-Only Memory)。可选地,该存储器包括非瞬时性计算机可读介质(non-transitory computer-readable storage medium)。存储器可用于存储指令、程序、代码、代码集或指令集。存储器可包括存储程序区和存储数据区,其中,存储程序区可存储用于实现操作系统的指令、用于至少一个功能的指令、用于实现上述各个方法实施例的指令等;存储数据区可存储根据服务器的使用所创建的数据等。

[0159] 处理器可以包括一个或者多个处理核心。处理器利用各种接口和线路连接整个服务器内的各个部分,通过运行或执行存储在存储器内的指令、程序、代码集或指令集,以及调用存储在存储器内的数据,执行服务器的各种功能和处理数据。可选地,处理器可以采用数字信号处理(Digital Signal Processing,DSP)、现场可编程门阵列(Field—Programmable Gate Array,FPGA)、可编程逻辑阵列(Programmable Logic Array,PLA)中的至少一种硬件形式来实现。处理器可集成中央处理器(Central Processing Unit,CPU)和调制解调器等中的一种或几种的组合。其中,CPU主要处理操作系统和应用程序等;调制解调器用于处理无线通信。可以理解的是,上述调制解调器也可以不集成到处理器中,单独通过一块芯片进行实现。

[0160] 由于该电子设备是本发明实施例的带隐私保护的一致性最优控制方法对应的电子设备,并且该电子设备解决问题的原理与该方法相似,因此该电子设备的实施可以参见上述方法实施例的实施过程,重复之处不再赘述。

[0161] 基于同一发明构思,本发明实施例还提供一种计算机可读存储介质,所述存储介质中存储有至少一条指令、至少一段程序、代码集或指令集,所述至少一条指令、所述至少一段程序、所述代码集或指令集由处理器加载并执行以实现如上所述的带隐私保护的一致性最优控制方法。

[0162] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储介质中,存储介质包括只读存储器(Read-Only Memory,ROM)、随机存储器(Random Access Memory,RAM)、可编程只读存储器(Programmable Read-only Memory,PROM)、可擦除可编程只读存储器(Erasable Programmable Read Only Memory,EPROM)、一次可编程只读存储器(One-time Programmable Read-Only Memory,OTPROM)、电子抹除式可复写只读存储器(Electrically-Erasable Programmable Read-Only Memory,EEPROM)、只读光盘(Compact Disc Read-Only Memory,CD-ROM)或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的计算机可读的任何其他介质。

[0163] 由于该存储介质是本发明实施例的带隐私保护的一致性最优控制方法对应的存储介质,并且该存储介质解决问题的原理与该方法相似,因此该存储介质的实施可以参见上述方法实施例的实施过程,重复之处不再赘述。

[0164] 在一些可能的实施方式中,本发明实施例的方法的各个方面还可以实现为一种程序产品的形式,其包括程序代码,当程序产品在计算机设备上运行时,程序代码用于使计算机设备执行本说明书上述描述的根据本申请各种示例性实施方式的带隐私保护的一致性

最优控制方法的步骤。其中，用于执行各个实施例的可执行的计算机程序代码或“ 代码”可以用诸如C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、结构化查询语言(例如，Transact-SQL)、Perl之类的高级编程语言或者用各种其它编程语言编写。

[0165] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0166] 上述实施例只是为了说明本发明的技术构思及特点，其目的是在于让本领域内的普通技术人员能够了解本发明的内容并据以实施，并不能以此限制本发明的保护范围。凡是根据本发明内容的实质所做出的等效的变化或修饰，都应涵盖在本发明的保护范围内。

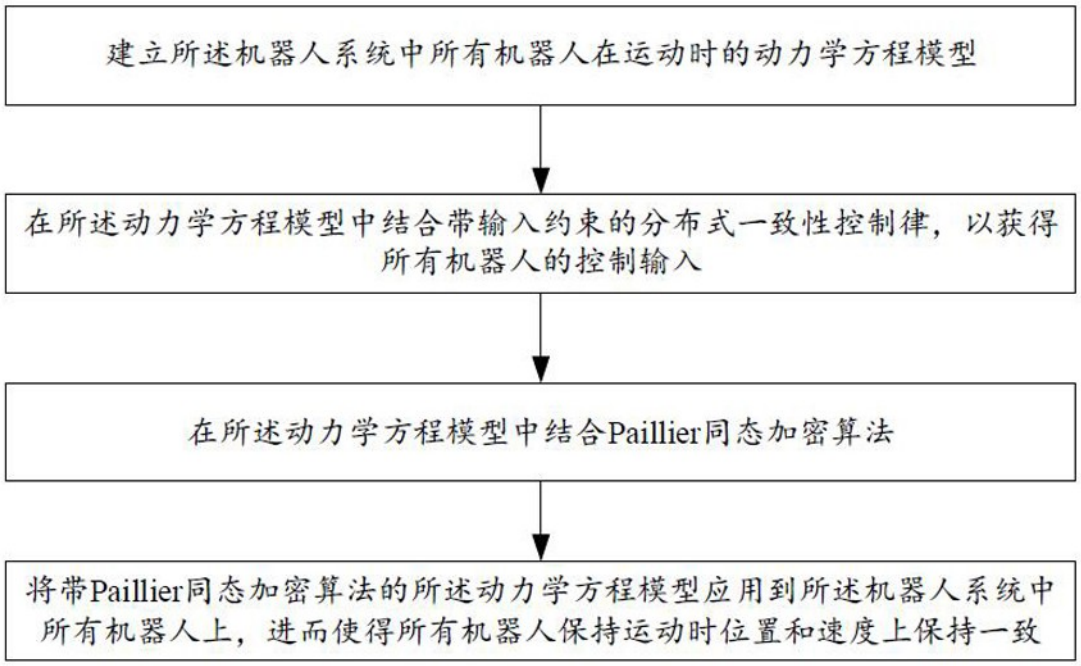

建立所述机器人系统中所有机器人在运动时的动力学方程模型
在所述动力学方程模型中结合带输入约束的分布式一致性控制律，以获得所有机器人的控制输入
在所述动力学方程模型中结合Paillier同态加密算法
将带Paillier同态加密算法的所述动力学方程模型应用到所述机器人系统中所有机器人上，进而使得所有机器人保持运动时位置和速度上保持一致

图1

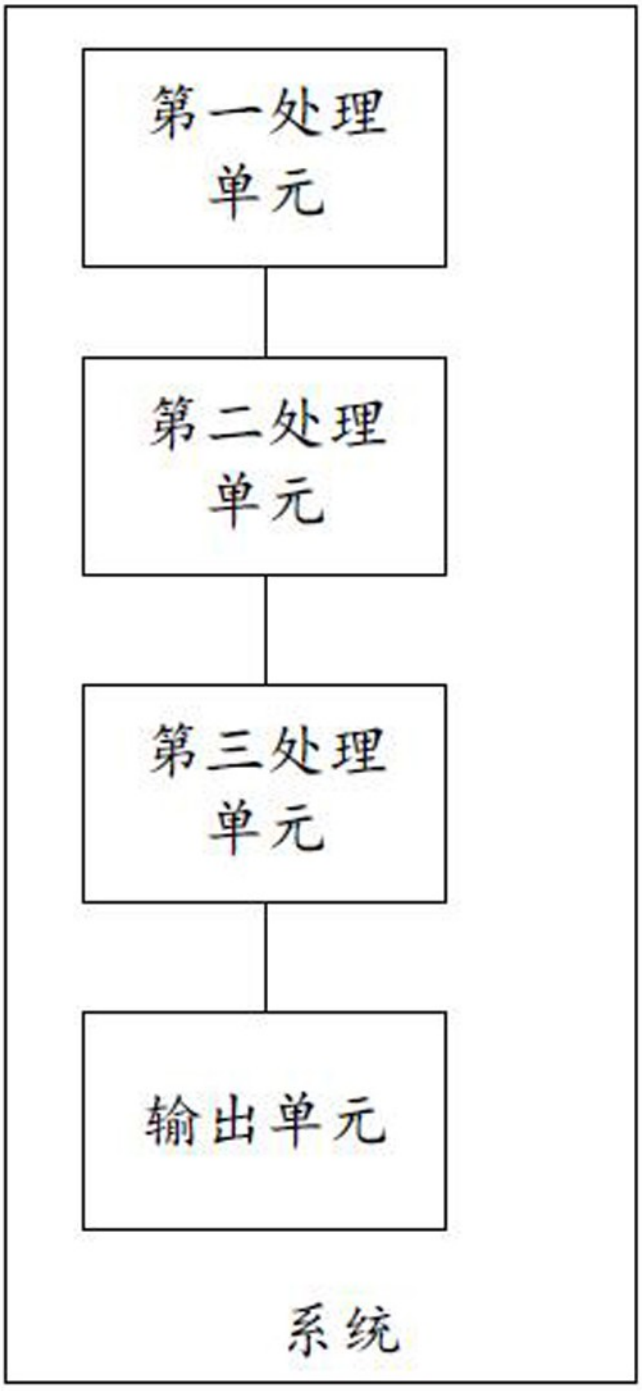


图2

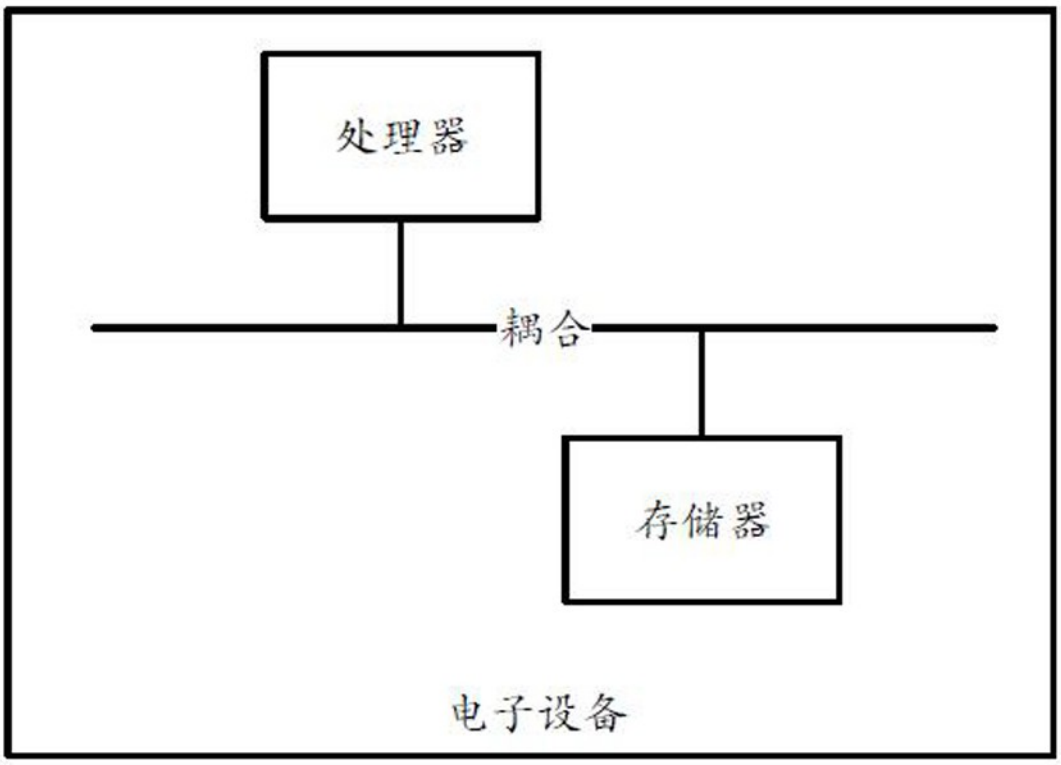


图3