(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 113779615 B
(45)授权公告日 2022.02.25

(21)申请号 202111344472.5

(22)申请日 2021.11.15

(65)同一申请的已公布的文献号
申请公布号 CN 113779615 A

(43)申请公布日 2021.12.10

(73)专利权人 蓝象智联(杭州)科技有限公司
地址 311100 浙江省杭州市余杭区西溪艺术村水墨西溪3号

(72)发明人 裴阳 刘洋 毛仁歆 徐时峰 朱振超

(74)专利代理机构 杭州天麟知识产权代理事务所(特殊普通合伙) 33374
代理人 占宇

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06N 3/04(2006.01)
G06N 3/08(2006.01)

(56)对比文件
CN 113344222 A,2021.09.03
CN 113169957 A,2021.07.23
天下客.《论文笔记:IJCAI 2021 Decentralized Federated Graph Neural Networks》.《知乎》.2021,第1-9页.

审查员 胡学岭

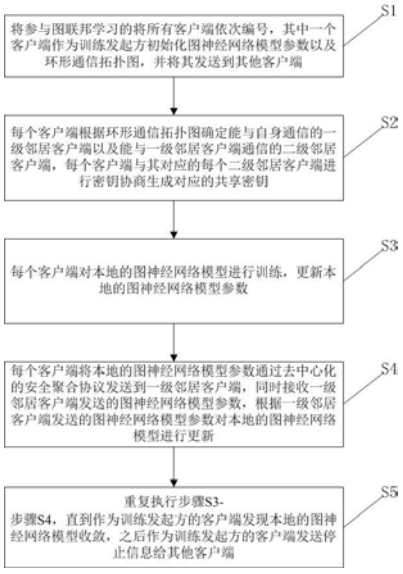
权利要求书2页 说明书8页 附图2页

(54)发明名称

一种安全的去中心化的图联邦学习方法

(57)摘要

本发明公开了一种安全的去中心化的图联邦学习方法。它包括以下步骤:S1:将所有客户端依次编号,初始化图神经网络模型参数以及环形通信拓扑图发送到所有客户端;S2:每个客户端根据环形通信拓扑图确定一级邻居客户端、二级邻居客户端,并与其对应的每个二级邻居客户端进行密钥协商生成对应的共享密钥;S3:每个客户端对本地的图神经网络模型进行训练,更新本地的图神经网络模型参数;S4:每个客户端接收一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新;S5:重复执行步骤S3-步骤S4,直到图神经网络模型收敛。本发明能够保护各个客户端的数据隐私和安全,减轻通信瓶颈,减少通信时间。



CN 113779615 B

1.一种安全的去中心化的图联邦学习方法,其特征在于,包括以下步骤:

S1:将参与图联邦学习的所有n个客户端依次编号为1、2、3……n,其中一个客户端作为训练发起方初始化图神经网络模型参数以及环形通信拓扑图,并将其发送到其他客户端;

S2:每个客户端根据环形通信拓扑图确定能与自身通信的一级邻居客户端以及能与一级邻居客户端通信的二级邻居客户端,每个客户端与其对应的每个二级邻居客户端进行密钥协商生成对应的共享密钥;

S3:每个客户端对本地的图神经网络模型进行训练,更新本地的图神经网络模型参数;

S4:每个客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到一级邻居客户端,同时接收一级邻居客户端发送的图神经网络模型参数,根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新;

S5:重复执行步骤S3-步骤S4,直到所有客户端本地的图神经网络模型收敛;

所述步骤S1中的环形通信拓扑图为矩阵A,

$$A=\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix},$$

$A_{i,j} \in [0,1]$, $\sum_{j=1}^{n} A_{i,j} = 1$, $A_{i,j} = A_{j,i}$,1≤i≤n,1≤j≤n,

当i=j时,$A_{ij}\neq 0$,

其中,A_{ij}表示编号为i的客户端与编号为j的客户端之间的权重系数,如果$A_{ij}\neq 0$表示编号为i的客户端与编号为j的客户端能够通信,如果$A_{ij}=0$表示编号为i的客户端与编号为j的客户端不能够通信;

所述步骤S2中某个编号为u的客户端与其对应的一个编号为v的二级邻居客户端进行密钥协商生成对应的共享密钥的方法包括以下步骤,1≤u≤n,1≤v≤n:

N1:编号为u的客户端与编号为v的二级邻居客户端根据预设的安全参数k,并使用KA.param算法生成Diffle-Hellman协议的公共参数pp;

N2:编号为u的客户端使用KA.gen算法和公共参数pp生成公钥私钥对(s_u^{PK}, s_u^{SK}),将公钥s_u^{PK}发送给编号为v的二级邻居客户端,

编号为v的二级邻居客户端使用KA.gen算法和公共参数pp生成公钥私钥对(s_v^{PK}, s_v^{SK}),将公钥s_v^{PK}发送给编号为u的客户端;

N3:编号为u的客户端根据KA.agree算法、私钥s_u^{SK}、公钥s_v^{PK}计算出共享密钥s_{uv},$KA.agree(s_u^{SK}, s_v^{PK}) \rightarrow s_{uv}$,编号为v的二级邻居客户端根据KA.agree算法、私钥s_v^{SK}、公钥s_u^{PK}计算出共享密钥s_{vu},$KA.agree(s_v^{SK}, s_u^{PK}) \rightarrow s_{vu}$,由于公钥私钥对$(s_u^{PK}, s_u^{SK})$与公钥私钥对$(s_v^{PK}, s_v^{SK})$都由同一个公共参数pp生成,所以$s_{uv}=s_{vu}$;

所述步骤S4中客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到某个一级邻居客户端的方法包括以下步骤:

客户端找出能与该一级邻居客户端通信的二级邻居客户端，并找出与该二级邻居客户端进行密钥协商生成的共享密钥，根据该共享密钥生成对应的加密噪声向量，将本地的图神经网络模型参数乘以该客户端与该一级邻居客户端之间的权重系数后再加上该加密噪声向量生成加密图神经网络模型参数，将该加密图神经网络模型参数发送到该一级邻居客户端；

某个编号为u的客户端根据与编号为v的二级邻居客户端协商生成的共享密钥生成对应的加密噪声向量的方法包括以下步骤，1≤u≤n，1≤v≤n：

编号为u的客户端将共享密钥s_{uv}输入伪随机数生成器PRG，生成加密噪声向量p_{uv}，$p_{uv}=\Delta_{uv}*PRG(s_{uv})$，其中，当u＞v时，$\Delta_{uv}=1$，当u＜v时，$\Delta_{uv}=-1$；

某个编号为u的客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到编号为w的一级邻居客户端的方法包括以下步骤，1≤w≤n：

编号为u的客户端找出能与编号为w的一级邻居客户端通信的编号为f的二级邻居客户端，1≤f≤n，找出与编号为f的二级邻居客户端进行密钥协商生成的加密噪声向量p_{uf}，编号为u的客户端将本地的图神经网络模型参数x_u乘以权重系数A_{uw}，再加上该加密噪声向量p_{uf}生成加密图神经网络模型参数$\overline{x_{uw}}$，$\overline{x_{uw}}=A_{uw}*x_u+p_{uf}$，并将其发送给编号为w的一级邻居客户端；

所述步骤S4中客户端接收一级邻居客户端发送的图神经网络模型参数，根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新的方法包括以下步骤：

客户端接收每个一级邻居客户端发送的加密图神经网络模型参数，将本地的图神经网络模型参数乘以自身的权重系数后再与所有接收到的加密图神经网络模型参数相加求和，得到新的图神经网络模型参数，并使用该新的图神经网络模型参数对本地的图神经网络模型进行更新；

某个编号为u的客户端接收编号为w的一级邻居客户端、编号为z的一级邻居客户端发送的图神经网络模型参数，根据编号为w的一级邻居客户端、编号为z的一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新的方法包括以下步骤，1≤z≤n：

编号为u的客户端接收到编号为w的一级邻居客户端发送的加密图神经网络模型参数$\overline{x_{wu}}=A_{wu}*x_w+p_{wz}$，接收到编号为z的一级邻居客户端发送的加密图神经网络模型参数$\overline{x_{zu}}=A_{zu}*x_z+p_{zw}$，编号为u的客户端计算出新的图神经网络模型参数$\overline{x_u}=A_{uu}*x_u+A_{wu}*x_w+p_{wz}+A_{zu}*x_z+p_{zw}$，由于$p_{wz}+p_{zw}=0$，所以$\overline{x_u}=A_{uu}*x_u+A_{wu}*x_w+A_{zu}*x_z$。

一种安全的去中心化的图联邦学习方法

技术领域

[0001] 本发明涉及图联邦学习技术领域，尤其涉及一种安全的去中心化的图联邦学习方法。

背景技术

[0002] 在过去的几年中，神经网络的兴起与应用成功推动了模式识别和数据挖掘的研究。传统的深度学习方法在提取欧氏空间数据特征方面取得了巨大的成功，但实际场景中的数据很多都是从非欧式空间生成的数据，深度学习方法在此类数据上的表现难以令人满意，如图网络中每个节点的邻居节点的个数是不固定的，导致一些重要操作(例如卷积)在图像上很容易计算，但不再适合直接用于图。并且深度学习基于训练数据满足独立同分布的假设之上，样本之间不存在相互依赖关系，而图结构数据最大的特点便是不同节点之间存在许多相互依赖联系，这就导致了深度学习无法挖掘图数据的内在联系。针对于此类数据，图神经网络技术应运而生。此外，在数据日益增加，数据联系日益紧密的今天，由于用户隐私和法律法规等问题，许多数据之间不能互通，产生了许多“数据孤岛”。联邦学习(Federated Learning)这一概念由Google在2017年提出，旨在于解决跨设备之间的联合建模问题，该方案为上述问题提供了一种可行的解法。

[0003] 目前的图联邦学习方案大多是基于Google提出的FedAvg算法上实现，系统结构由一个中心服务器和若干个客户端组成，中心服务器提供全局共享的模型，各客户端下载模型并在本地数据集上训练，更新本地模型参数，然后将更新后的模型参数发送给中心服务器聚合，中心服务器聚合后得到本次迭代的模型更新值，进行全局模型参数更新；以此循环。上述方案在全局模型聚合阶段客户端并未对发送到中心服务器的本地模型参数进行保护，以防止可能存在的信息泄漏；其次，负责聚合模型信息的中心服务器端要求是可信的中立的第三方机构，对于机构之间建模，这种可信的中立的第三方是很难保证的；最后，这种中心化的架构对中心服务器端的IO能力提出了很高的要求，所有客户端都必须等待全部客户端将模型参数上传中心服务器成功，然后中心服务器将更新后的全局模型参数分发至客户端，客户端才能进行下一次循环，这无疑是十分消耗时间的。

发明内容

[0004] 本发明为了解决上述技术问题，提供了一种安全的去中心化的图联邦学习方法，其采用了去中心化的环形拓扑结构，移除了收集客户端模型信息的中心服务器节点，模型参数的通信进行了加密，保护了各个客户端的数据隐私和安全，减轻了通信瓶颈，减少了通信时间。

[0005] 为了解决上述问题，本发明采用以下技术方案予以实现：

[0006] 本发明的一种安全的去中心化的图联邦学习方法，包括以下步骤：

[0007] S1：将参与图联邦学习的所有n个客户端依次编号为1、2、3……n，其中一个客户端作为训练发起方初始化图神经网络模型参数以及环形通信拓扑图，并将其发送到其他客户

端；

[0008] S2：每个客户端根据环形通信拓扑图确定能与自身通信的一级邻居客户端以及能与一级邻居客户端通信的二级邻居客户端，每个客户端与其对应的每个二级邻居客户端进行密钥协商生成对应的共享密钥；

[0009] S3：每个客户端对本地的图神经网络模型进行训练，更新本地的图神经网络模型参数；

[0010] S4：每个客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到一级邻居客户端，同时接收一级邻居客户端发送的图神经网络模型参数，根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新；

[0011] S5：重复执行步骤S3-步骤S4，直到所有客户端本地的图神经网络模型收敛。

[0012] 在本方案中，参与图联邦学习的所有n个客户端根据环形通信拓扑图组成环形拓扑结构，n≥3，每个客户端都有两个一级邻居客户端，每个一级邻居客户端都对应有一个能够与自身通信的二级邻居客户端，即每个客户端都有两个二级邻居客户端。每个客户端都与它的每个二级邻居客户端进行密钥协商生成对应的共享密钥，即每个客户端会生成两个共享密钥，分别与两个二级邻居客户端对应。每个客户端要将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到两个一级邻居客户端，同时接收这两个一级邻居客户端发送的图神经网络模型参数，根据这两个一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新。所有n个客户端组成环形拓扑结构，每个客户端每次迭代后都可以学习到邻居客户端的图神经网络模型参数，假设离客户端g最远的客户端需要经过D个邻居客户端到达，那么经过D+1次迭代，客户端g就能学习到所有客户端的图神经网络模型参数。

[0013] 本方案中每个客户端通过去中心化的安全聚合协议对模型参数的发送进行加密，移除了收集客户端模型信息的中心服务器节点，保护了客户端的数据隐私和安全，每个客户端都根据两个一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新，由于所有客户端组成环形拓扑结构，所以本方案的通信负载均衡，其他图联邦学习方案中是一个服务器对多个客户端通信，通信时服务器端通信IO压力很大，本方案中将通信平均到每个客户端，减轻了通信瓶颈，减少了通信时间。

[0014] 作为优选，所述步骤S1中的环形通信拓扑图为矩阵A，

[0015] $$\mathrm{A}=\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix},$$

[0016] $A_{i,j} \in [0,1]$，$\sum_{j=1}^{n} A_{i,j} = 1$，$A_{i,j} = A_{j,i}$，1≤i≤n，1≤j≤n，

[0017] 当i=j时，$A_{ij} \neq 0$，

[0018] 其中，A_{ij}表示编号为i的客户端与编号为j的客户端之间的权重系数，如果$A_{ij} \neq 0$表示编号为i的客户端与编号为j的客户端能够通信，如果$A_{ij}=0$表示编号为i的客户端与编号为j的客户端不能够通信。

[0019] 矩阵A是一个对称的矩阵。A_{ii}表示编号为i的客户端自身的权重系数。

$\sum_{j=1}^{n} A_{i,j} = 1$表示矩阵A的每一行的和为1。

[0020] 作为优选，所述步骤S2中某个编号为u的客户端与其对应的一个编号为v的二级邻居客户端进行密钥协商生成对应的共享密钥的方法包括以下步骤，1≤u≤n，1≤v≤n：

[0021] N1：编号为u的客户端与编号为v的二级邻居客户端根据预设的安全参数k，并使用KA.param算法生成Diffle-Hellman协议的公共参数pp，

[0022] $KA.param(k) \rightarrow pp$；

[0023] N2：编号为u的客户端使用KA.gen算法和公共参数pp生成公钥私钥对(s_u^{PK}, s_u^{SK})，$KA.gen(pp) \rightarrow (s_u^{PK}, s_u^{SK})$，将公钥$s_u^{PK}$发送给编号为v的二级邻居客户端，

[0024] 编号为v的二级邻居客户端使用KA.gen算法和公共参数pp生成公钥私钥对(s_v^{PK}, s_v^{SK})，$KA.gen(pp) \rightarrow (s_v^{PK}, s_v^{SK})$，将公钥$s_v^{PK}$发送给编号为u的客户端；

[0025] N3：编号为u的客户端根据KA.agree算法、私钥s_u^{SK}、公钥s_v^{PK}计算出共享密钥s_{uv}，$KA.agree(s_u^{SK}, s_v^{PK}) \rightarrow s_{uv}$，编号为v的二级邻居客户端根据KA.agree算法、私钥s_v^{SK}、公钥s_u^{PK}计算出共享密钥s_{vu}，$KA.agree(s_v^{SK}, s_u^{PK}) \rightarrow s_{vu}$，由于公钥私钥对$(s_u^{PK}, s_u^{SK})$与公钥私钥对$(s_v^{PK}, s_v^{SK})$都由同一个公共参数pp生成，所以$s_{uv}=s_{vu}$。

[0026] 作为优选，所述步骤S4中客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到某个一级邻居客户端的方法包括以下步骤：

[0027] 客户端找出能与该一级邻居客户端通信的二级邻居客户端，并找出与该二级邻居客户端进行密钥协商生成的共享密钥，根据该共享密钥生成对应的加密噪声向量，将本地的图神经网络模型参数乘以该客户端与该一级邻居客户端之间的权重系数后再加上该加密噪声向量生成加密图神经网络模型参数，将该加密图神经网络模型参数发送到该一级邻居客户端。

[0028] 作为优选，某个编号为u的客户端根据与编号为v的二级邻居客户端协商生成的共享密钥生成对应的加密噪声向量的方法包括以下步骤，1≤u≤n，1≤v≤n：

[0029] 编号为u的客户端将共享密钥s_{uv}输入伪随机数生成器PRG，生成加密噪声向量p_{uv}，$p_{uv} = \Delta_{uv} * PRG(s_{uv})$，其中，当u＞v时，$\Delta_{uv} = 1$，当u＜v时，$\Delta_{uv} = -1$，即$p_{uv}+p_{vu}=0$。

[0030] 某个编号为u的客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到编号为w的一级邻居客户端的方法包括以下步骤，1≤w≤n：

[0031] 编号为u的客户端找出能与编号为w的一级邻居客户端通信的编号为f的二级邻居客户端，1≤f≤n，找出与编号为f的二级邻居客户端进行密钥协商生成的加密噪声向量p_{uf}，编号为u的客户端将本地的图神经网络模型参数x_u乘以权重系数A_{uw}，再加上该加密噪声向量p_{uf}生成加密图神经网络模型参数$\overline{x_{uw}}$，$\overline{x_{uw}} = A_{uw} * x_u + p_{uf}$，并将其发送给编号为w的一级邻居客户端。

[0032] 作为优选，所述步骤S4中客户端接收一级邻居客户端发送的图神经网络模型参数，根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新的

方法包括以下步骤：

[0033] 客户端接收每个一级邻居客户端发送的加密图神经网络模型参数，将本地的图神经网络模型参数乘以自身的权重系数后再与所有接收到的加密图神经网络模型参数相加求和，得到新的图神经网络模型参数，并使用该新的图神经网络模型参数对本地的图神经网络模型进行更新。

[0034] 某个编号为u的客户端接收编号为w的一级邻居客户端、编号为z的一级邻居客户端发送的图神经网络模型参数，根据编号为w的一级邻居客户端、编号为z的一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新的方法包括以下步骤，1≤z≤n：

[0035] 编号为u的客户端接收到编号为w的一级邻居客户端发送的加密图神经网络模型参数$\overline{x_{wu}} = A_{wu} * x_w + p_{wz}$，接收到编号为z的一级邻居客户端发送的加密图神经网络模型参数$\overline{x_{zu}} = A_{zu} * x_z + p_{zw}$，编号为u的客户端计算出新的图神经网络模型参数$\overline{x_u} = A_{uu} * x_u + A_{wu} * x_w + p_{wz} + A_{zu} * x_z + p_{zw}$，由于$p_{wz}+p_{zw}=0$，所以$\overline{x_u} = A_{uu} * x_u + A_{wu} * x_w + A_{zu} * x_z$。

[0036] 这里编号为u的客户端分别能够与编号为w的客户端、编号为z的客户端通信，所以编号为u的客户端也是编号为w的客户端的一级邻居客户端，编号为z的客户端是能够与编号为u的一级邻居客户端通信的二级邻居客户端，所以编号为w的一级邻居客户端发送给编号为u的客户端的加密图神经网络模型参数为$\overline{x_{wu}} = A_{wu} * x_w + p_{wz}$，同理对于编号为z的客户端来说，编号为w的客户端是能够与编号为u的一级邻居客户端通信的二级邻居客户端。

[0037] 本发明的有益效果是：(1)采用了去中心化的环形拓扑结构，移除了收集客户端模型信息的中心服务器节点，模型参数的通信进行了加密，保护了各个客户端的数据隐私和安全。(2)将通信平均到每个客户端，减轻了通信瓶颈，减少了通信时间。

附图说明

[0038] 图1是实施例的流程图；

[0039] 图2是一种环形拓扑结构的结构示意图。

具体实施方式

[0040] 下面通过实施例，并结合附图，对本发明的技术方案作进一步具体的说明。

[0041] 实施例：本实施例的一种安全的去中心化的图联邦学习方法，如图1所示，包括以下步骤：

[0042] S1：将参与图联邦学习的所有n个客户端依次编号为1、2、3……n，其中一个客户端作为训练发起方初始化图神经网络模型参数以及环形通信拓扑图，并将其发送到其他客户端；

[0043] 环形通信拓扑图为矩阵A，

[0044] $$A=\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix},$$

[0045] $A_{i,j} \in [0,1]$, $\sum_{j=1}^{n} A_{i,j} = 1$, $A_{i,j} = A_{j,i}$,1≤i≤n,1≤j≤n,

[0046] 当i=j时,$A_{ij}\neq 0$,

[0047] 其中,A_{ij}表示编号为i的客户端与编号为j的客户端之间的权重系数,如果$A_{ij}\neq 0$表示编号为i的客户端与编号为j的客户端能够通信,如果$A_{ij}=0$表示编号为i的客户端与编号为j的客户端不能够通信,矩阵A是一个对称的矩阵,A_{ii}表示编号为i的客户端自身的权重系数,$\sum_{j=1}^{n} A_{i,j} = 1$表示矩阵A的每一行的和为1;

[0048] S2:每个客户端根据环形通信拓扑图确定能与自身通信的一级邻居客户端以及能与一级邻居客户端通信的二级邻居客户端,每个客户端与其对应的每个二级邻居客户端进行密钥协商生成对应的共享密钥;

[0049] 某个编号为u的客户端与其对应的一个编号为v的二级邻居客户端进行密钥协商生成对应的共享密钥的方法包括以下步骤,1≤u≤n,1≤v≤n:

[0050] N1:编号为u的客户端与编号为v的二级邻居客户端根据预设的安全参数k(安全参数k是所有客户端都共同持有,并且保持一致),并使用KA.param算法生成Diffle-Hellman协议的公共参数pp,

[0051] $KA.param(k) \rightarrow pp$;

[0052] N2:编号为u的客户端使用KA.gen算法和公共参数pp生成公钥私钥对(s_u^{PK}, s_u^{SK}),$KA.gen(pp) \rightarrow (s_u^{PK}, s_u^{SK})$,将公钥$s_u^{PK}$发送给编号为v的二级邻居客户端,

[0053] 编号为v的二级邻居客户端使用KA.gen算法和公共参数pp生成公钥私钥对(s_v^{PK}, s_v^{SK}),$KA.gen(pp) \rightarrow (s_v^{PK}, s_v^{SK})$,将公钥$s_v^{PK}$发送给编号为u的客户端;

[0054] N3:编号为u的客户端根据KA.agree算法、私钥s_u^{SK}、公钥s_v^{PK}计算出共享密钥s_{uv},$KA.agree(s_u^{SK}, s_v^{PK}) \rightarrow s_{uv}$,编号为v的二级邻居客户端根据KA.agree算法、私钥s_v^{SK}、公钥s_u^{PK}计算出共享密钥s_{vu},$KA.agree(s_v^{SK}, s_u^{PK}) \rightarrow s_{vu}$,由于公钥私钥对$(s_u^{PK}, s_u^{SK})$与公钥私钥对$(s_v^{PK}, s_v^{SK})$都由同一个公共参数pp生成,所以$s_{uv}=s_{vu}$;

[0055] S3:每个客户端对本地的图神经网络模型进行训练,更新本地的图神经网络模型参数;

[0056] S4:每个客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到一级邻居客户端,同时接收一级邻居客户端发送的图神经网络模型参数,根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新;

[0057] 客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到某个一级邻居客户端的方法包括以下步骤:

[0058] 客户端找出能与该一级邻居客户端通信的二级邻居客户端,并找出与该二级邻居

客户端进行密钥协商生成的共享密钥，根据该共享密钥生成对应的加密噪声向量，将本地的图神经网络模型参数乘以该客户端与该一级邻居客户端之间的权重系数后再加上该加密噪声向量生成加密图神经网络模型参数，将该加密图神经网络模型参数发送到该一级邻居客户端；

[0059] 某个编号为u的客户端根据与编号为v的二级邻居客户端协商生成的共享密钥生成对应的加密噪声向量的方法包括以下步骤，1≤u≤n，1≤v≤n：

[0060] 编号为u的客户端将共享密钥s_{uv}输入伪随机数生成器PRG，生成加密噪声向量p_{uv}，$p_{uv}=\Delta_{uv}*PRG(s_{uv})$，其中，当u＞v时，$\Delta_{uv}=1$，当u＜v时，$\Delta_{uv}=-1$，由于$s_{uv}=s_{vu}$，$\Delta_{uv}=-\Delta_{vu}$，所以$p_{uv}+p_{vu}=0$；

[0061] 客户端接收一级邻居客户端发送的图神经网络模型参数，根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新的方法包括以下步骤：

[0062] 客户端接收每个一级邻居客户端发送的加密图神经网络模型参数，将本地的图神经网络模型参数乘以自身的权重系数后再与所有接收到的加密图神经网络模型参数相加求和，得到新的图神经网络模型参数，并使用该新的图神经网络模型参数对本地的图神经网络模型进行更新；

[0063] S5：重复执行步骤S3-步骤S4，直到作为训练发起方的客户端发现本地的图神经网络模型收敛，之后作为训练发起方的客户端发送停止信息给其他客户端。

[0064] 在本方案中，整个全局图为G=(V,E)，参与图联邦学习的每个客户端都持有全局图的部分子图，编号为i的客户端拥有的子图为$G_i=(V_i,E_i)\subset G$，每个客户端在本地子图上进行图神经网络模型训练，并更新本地图神经网络模型参数。

[0065] 参与图联邦学习的所有n个客户端根据环形通信拓扑图组成环形拓扑结构，n≥3，每个客户端都有两个一级邻居客户端，每个一级邻居客户端都对应有一个能够与自身通信的二级邻居客户端，即每个客户端都有两个二级邻居客户端。每个客户端都与它的每个二级邻居客户端进行密钥协商生成对应的共享密钥，即每个客户端会生成两个共享密钥，分别与两个二级邻居客户端对应。每个客户端要将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到两个一级邻居客户端，同时接收这两个一级邻居客户端发送的图神经网络模型参数，根据这两个一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新。重复执行上述步骤直到作为训练发起方的客户端发现本地的图神经网络模型收敛，作为训练发起方的客户端发现本地的图神经网络模型收敛后发送停止信息给其他客户端，参与图联邦学习的所有n个客户端停止图联邦学习。

[0066] 所有n个客户端组成环形拓扑结构，每个客户端每次迭代后都可以学习到邻居客户端的图神经网络模型参数，假设离客户端g最远的客户端需要经过D个邻居客户端到达，那么经过D+1次迭代，客户端g就能学习到所有客户端的图神经网络模型参数。由于所有n个客户端组成环形拓扑结构，每个客户端离最远的客户端的距离是一样的，所以当作为训练发起方的客户端发现本地的图神经网络模型收敛时，所有客户端本地的图神经网络模型都已经收敛。

[0067] 某个编号为u的客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到编号为w的一级邻居客户端的方法包括以下步骤，1≤w≤n：

[0068] 编号为u的客户端找出能与编号为w的一级邻居客户端通信的编号为f的二级邻居客户端，1≤f≤n，找出与编号为f的二级邻居客户端进行密钥协商生成的加密噪声向量p_{uf}，编号为u的客户端将本地的图神经网络模型参数x_u乘以权重系数A_{uw}，再加上该加密噪声向量p_{uf}生成加密图神经网络模型参数$\overline{x_{uw}}$，$\overline{x_{uw}} = A_{uw} * x_u + p_{uf}$，并将其发送给编号为w的一级邻居客户端。

[0069] 某个编号为u的客户端接收编号为w的一级邻居客户端、编号为z的一级邻居客户端发送的图神经网络模型参数，根据编号为w的一级邻居客户端、编号为z的一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新的方法包括以下步骤，1≤z≤n：

[0070] 编号为u的客户端接收到编号为w的一级邻居客户端发送的加密图神经网络模型参数$\overline{x_{wu}} = A_{wu} * x_w + p_{wz}$，接收到编号为z的一级邻居客户端发送的加密图神经网络模型参数$\overline{x_{zu}} = A_{zu} * x_z + p_{zw}$，编号为u的客户端计算出新的图神经网络模型参数$\overline{x_u} = A_{uu} * x_u + A_{wu} * x_w + p_{wz} + A_{zu} * x_z + p_{zw}$，由于$p_{wz}+p_{zw}=0$，所以$\overline{x_u} = A_{uu} * x_u + A_{wu} * x_w + A_{zu} * x_z$。由于$\sum_{j=1}^{n} A_{i,j} = 1$，$A_{i,j} = A_{j,i}$，所以$A_{uu} + A_{wu} + A_{zu} = 1$。

[0071] 这里编号为u的客户端分别能够与编号为w的客户端、编号为z的客户端通信，所以对于编号为w的客户端来说：编号为u的客户端也是编号为w的客户端的一级邻居客户端，编号为z的客户端是能够与编号为u的一级邻居客户端通信的二级邻居客户端，所以编号为w的一级邻居客户端发送给编号为u的客户端的加密图神经网络模型参数为$\overline{x_{wu}} = A_{wu} * x_w + p_{wz}$；同理对于编号为z的客户端来说：编号为w的客户端是能够与编号为u的一级邻居客户端通信的二级邻居客户端。

[0072] 本方案中每个客户端通过去中心化的安全聚合协议对模型参数的发送进行加密，移除了收集客户端模型信息的中心服务器节点，保护了客户端的数据隐私和安全，每个客户端都根据两个一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新，由于所有客户端组成环形拓扑结构，所以本方案的通信负载均衡，其他图联邦学习方案中是一个服务器对多个客户端通信，通信时服务器端通信IO压力很大，本方案中将通信平均到每个客户端，减轻了通信瓶颈，减少了通信时间。

[0073] 例如：如图2所示，参与图联邦学习的客户端有4个，依次编号为1、2、3、4，环形通信拓扑图为矩阵A，

[0074] $$A = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & 0 & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & 0 & \frac{1}{3} & \frac{1}{3} \end{bmatrix},$$

[0075] 客户端1的一级邻居客户端是客户端2、客户端4，客户端3是能与一级邻居客户端2通信的二级邻居客户端，客户端3也是能与一级邻居客户端4通信的二级邻居客户端，客户

端1与客户端3进行密钥协商，客户端2与客户端4进行密钥协商。

[0076] 客户端1向一级邻居客户端2发送的加密图神经网络模型参数为$\overline{x_{12}}=\frac{1}{3}*x_1+p_{13}$，向一级邻居客户端4发送的加密图神经网络模型参数为$\overline{x_{14}}=\frac{1}{3}*x_1+p_{13}$，客户端1接收到一级邻居客户端2发送的加密图神经网络模型参数为$\overline{x_{21}}=\frac{1}{3}*x_2+p_{24}$，客户端1接收到一级邻居客户端4发送的加密图神经网络模型参数为$\overline{x_{41}}=\frac{1}{3}*x_4+p_{42}$，客户端1计算出新的图神经网络模型参数$\overline{x_1}=\frac{1}{3}*x_1+\frac{1}{3}*x_2+p_{24}+\frac{1}{3}*x_4+p_{42}=\frac{x_1+x_2+x_4}{3}$，使用该新的图神经网络模型参数对本地的图神经网络模型进行更新。

[0077] 4个客户端组成环形拓扑结构，每个客户端每次迭代后都可以学习到邻居客户端的图神经网络模型参数，离每个客户端最远的客户端都需要经过1个邻居到达，那么经过2次迭代，每个客户端就能学习到所有客户端的图神经网络模型参数。

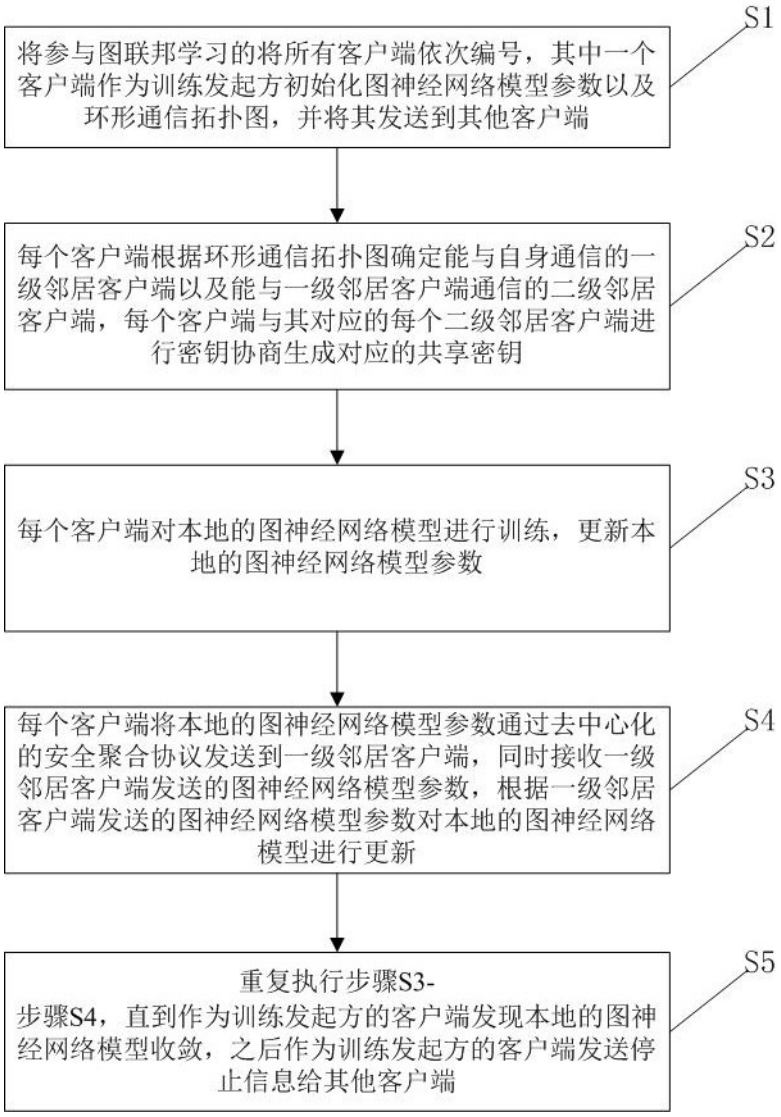

S1
将参与图联邦学习的将所有客户端依次编号，其中一个客户端作为训练发起方初始化图神经网络模型参数以及环形通信拓扑图，并将其发送到其他客户端
S2
每个客户端根据环形通信拓扑图确定能与自身通信的一级邻居客户端以及能与一级邻居客户端通信的二级邻居客户端，每个客户端与其对应的每个二级邻居客户端进行密钥协商生成对应的共享密钥
S3
每个客户端对本地的图神经网络模型进行训练，更新本地的图神经网络模型参数
S4
每个客户端将本地的图神经网络模型参数通过去中心化的安全聚合协议发送到一级邻居客户端，同时接收一级邻居客户端发送的图神经网络模型参数，根据一级邻居客户端发送的图神经网络模型参数对本地的图神经网络模型进行更新
S5
重复执行步骤S3-
步骤S4，直到作为训练发起方的客户端发现本地的图神经网络模型收敛，之后作为训练发起方的客户端发送停止信息给其他客户端

图1

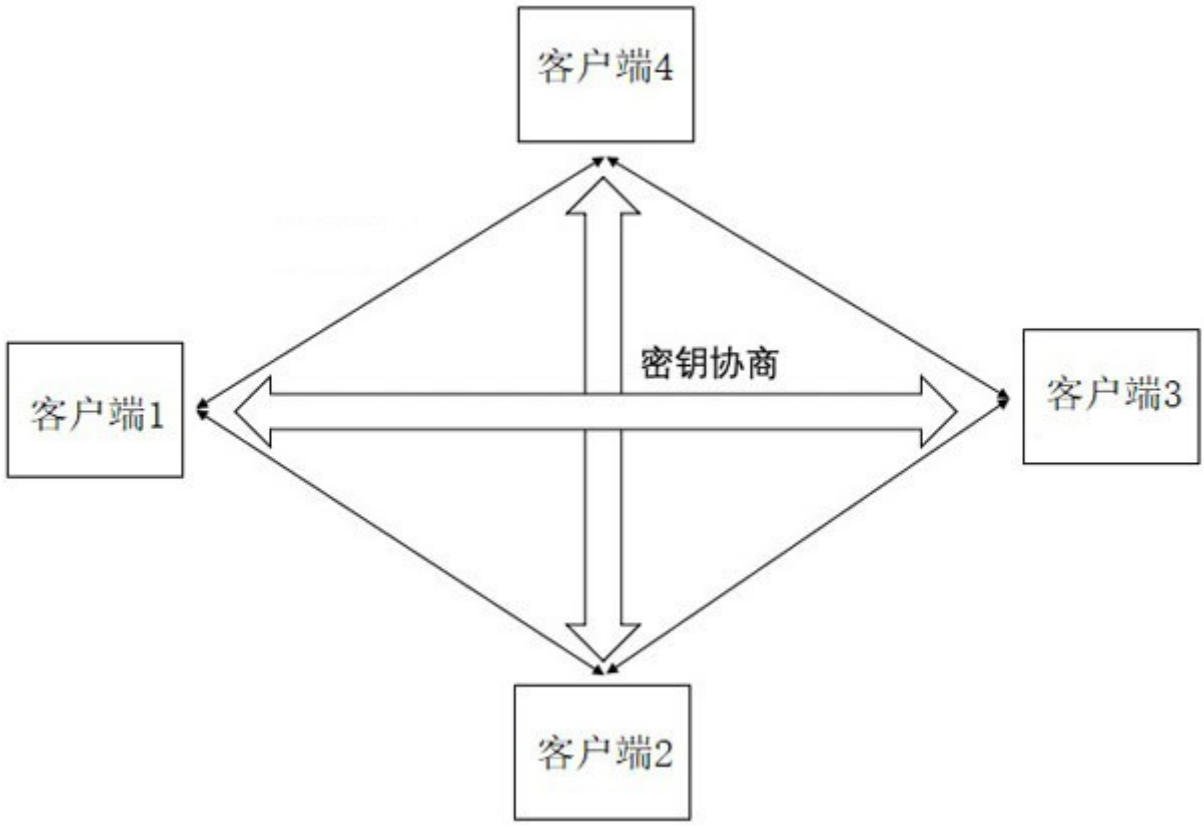


图2