PIRATE:5G网络中基于区块链的分布式机器学习安全框架

基于区块链的分布式机器学习保护框架：PIRATE，并以分散的方式进行管理。为了保护梯度聚合和模型参数，提出的方法利用了基于分片的区块链协议和梯度异常检测，可以消除产生有害梯度的恶意节点的工作。

具体实现：

权限/访问控制

在实际参与全局学习任务之前，所有节点都由一个集中的组件根据其计算能力、网络状况、加入/离开前景和历史信用分数进行评估。节点一旦获得许可，就可以加入委员会。

在训练期间，由委员会生成的经验证的信用分数被传输到许可控制中心。累积信用分数较低的节点将被逐出系统。

面向分散式学习的基于分片的区块链保护

将计算节点随机分为多个委员会，经委员会成员同意进行模型参数聚合。

局部梯度聚合-结果验证-成员签名-传输给邻居委员会。

委员会内部共识

局部梯度选择：

委员会成员可以合作选择c2/n局部梯度，或者以循环方式协调以选择c2/n局部梯度。有了邻居委员会聚合和一组局部梯度，领导者和成员都可以使用基于检测的BFT聚合来聚合它们。
预训练异常检测模型将根据异常得分为每个梯度分配权重。如果异常评分超过阈值，将相应地分配零权重，从而过滤阻碍收敛的有害梯度。同时，在新的委员会成立之前，成员必须存储彼此的历史信用分数。在委员会重新配置之前，信用评分会传输到权限控制中心。

邻居委员会聚合：

成员们等待邻居委员会的领导人广播上一步的防篡改邻居聚合。

聚合结果：

现任领导广播训练参数的部分聚合和散列索引，供成员验证和同意。如果有足够的法定人数证书，领导将在委员会和邻接委员会中广播决定的集合。如果领导选择向邻居委员会隐瞒结果，邻居委员会可以向随机的委员会成员索要结果。

未解决的问题：

分散的权限控制

不能抵抗模型中毒攻击