Notes for SL (ch)

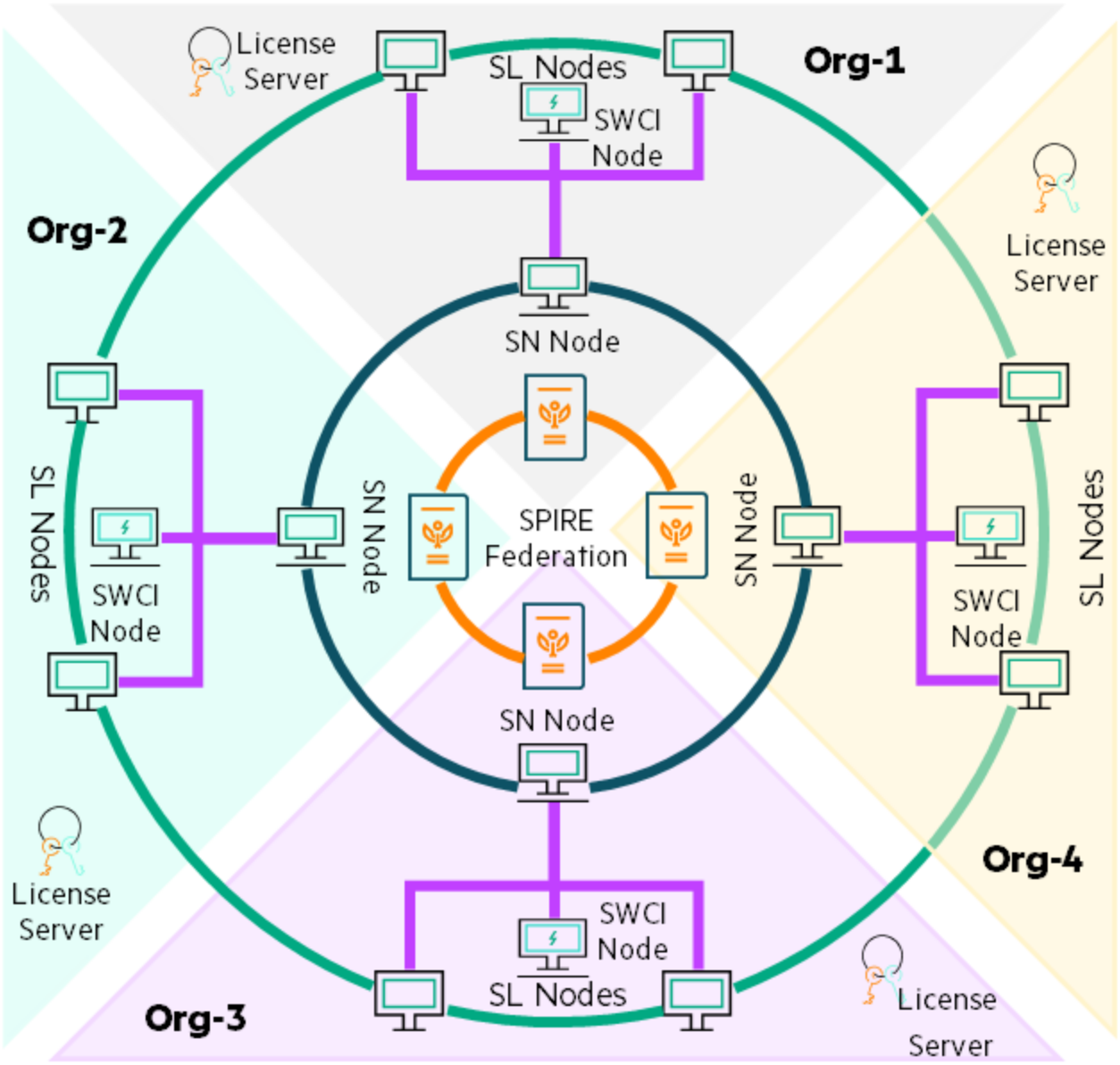
Introduction

SL是一种分布式的，隐私保护机器学习框架；

该框架使用数据源本身或周边的算力驱动机器学习模型的训练；

使用区块链安全地分享学习成果；

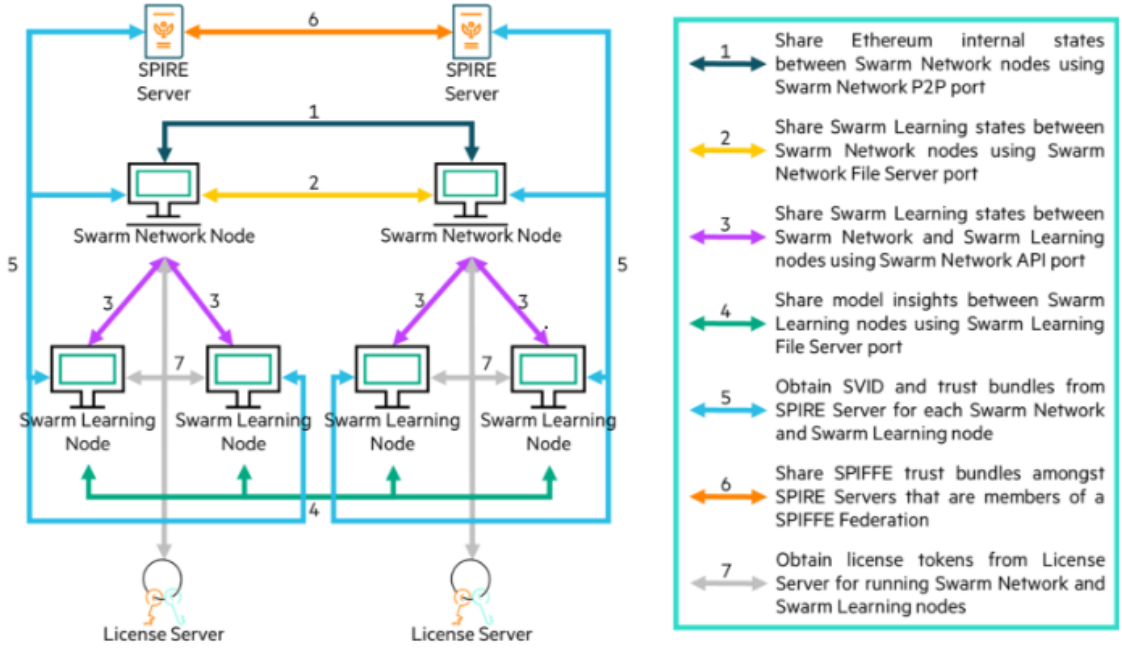
Components



SL网络由5种组件构成：

- **Swarm Learning nodes**：负责模型的训练和更新；
- **Swarm Network nodes**：负责基于区块链服务维护全局模型状态，追踪事务（只有元数据会被写入区块链，模型本身不会存储在区块链中）；
  - Sentinel node：一个特殊的SN节点，第一个启动节点，用于初始化区块链网络；
- **Swarm Learning Command Interface node**：用于控制管理系统框架，查看系统状态；提供安全的连接以访问Swarm Network node；
- **SPIFFE SPIRE Server nodes**：负责整个网络的身份认证，多个节点可以构成一个认证联盟；
- **Licence Server node**：许可证节点配置并管理了准入该系统的许可证；

Components interactions



1. **SN p2p port**：用于SN节点分享以太坊内部状态信息；
2. **SN file server port**：用于SN节点分享关于Swarm Learning状态信息；
3. **SN API port**：用于SN节点与在该节点注册的SL节点分享Swarm Learning状态信息；
4. **SL file server port**：用于SL节点之间分享学习进度；
5. **SPIRE server API port**：用于SN节点和SL节点访问SPIRE节点以获取身份认证信息；
6. **SPIRE server federation port**：用于多个SPIRE server节点之间共识身份认证信息；
7. **Licence server API port**：用于SN节点和SL节点获取证书；

Working of a Swarm Learning node

一个SL节点如下工作：

1. 获取证书；
2. 从SPIRE server处获取身份认证；
3. 向一个SN节点注册；
4. 启动一个文件服务器并向SN节点声明已经准备好运行模型训练程序；

5. 启动用户定义的模型训练程序；

一个SL节点周期性地与其他SL节点共享学习进度，这个共享学习进度的周期称之为Synchronization Interval，这个参数决定了节点在多少批次的训练后分享学习进度。

注意：设定一个较大的同步周期可能会导致准确的下降；而设定一个较小的同步周期可能会导致频繁的同步，拖慢学习进程；

Swarm Learning可以动态调整同步周期，通过一个叫做mean loss的损失函数判断训练进程，mean loss的降低意味着良好的训练进程，就可以适当增大同步周期以加速训练进程；相反，如果训练进度不理想，就适当减小同步周期，使得节点之间更加频繁地共享参数；

在每一个同步周期的结尾，一个SL节点会被设计为admin，负责收集所有其他节点的模型然后聚合成一个模型，每个SL节点会使用这个聚合后的模型开始下一轮的训练。这个过程由SN节点协调；

机器学习算法可以设定一个最小节点阈值。当工作节点的数量小于阈值的时候，就暂停同步进程直到有达到阈值数量的工作节点；

一个SL节点维护两个输入输出目录：数据目录`/platform/swarmml/data`（输入）和模型目录`/platform/swarmml/model`（输入输出）；

*Remaining questions

- 是否允许存在作恶现象；
- 参数更新的共享是否加密；
- 对SL节点作恶的情况是否有惩罚机制；
- 对SL节点的模型训练贡献是否有激励机制；
- SN节点的维护方；
- 一轮训练后的聚合admin的选举机制；
- 模型更新的广播算法；
- 链上有关模型状态元数据的设计；

Reference

1. Warnat-Herresthal, Stefanie, et al. "Swarm learning for decentralized and confidential clinical machine learning." Nature 594.7862 (2021): 265-270.
2. Technical white paper. SWARM LEARNING: TURN YOUR DISTRIBUTED DATA INTO COMPETITIVE EDGE.
3. Warnat-Herresthal, Stefanie, et al. "Swarm Learning as a privacy-preserving machine learning approach for disease classification." BioRxiv (2020).
4. https://github.com/HewlettPackard/swarm-learning.