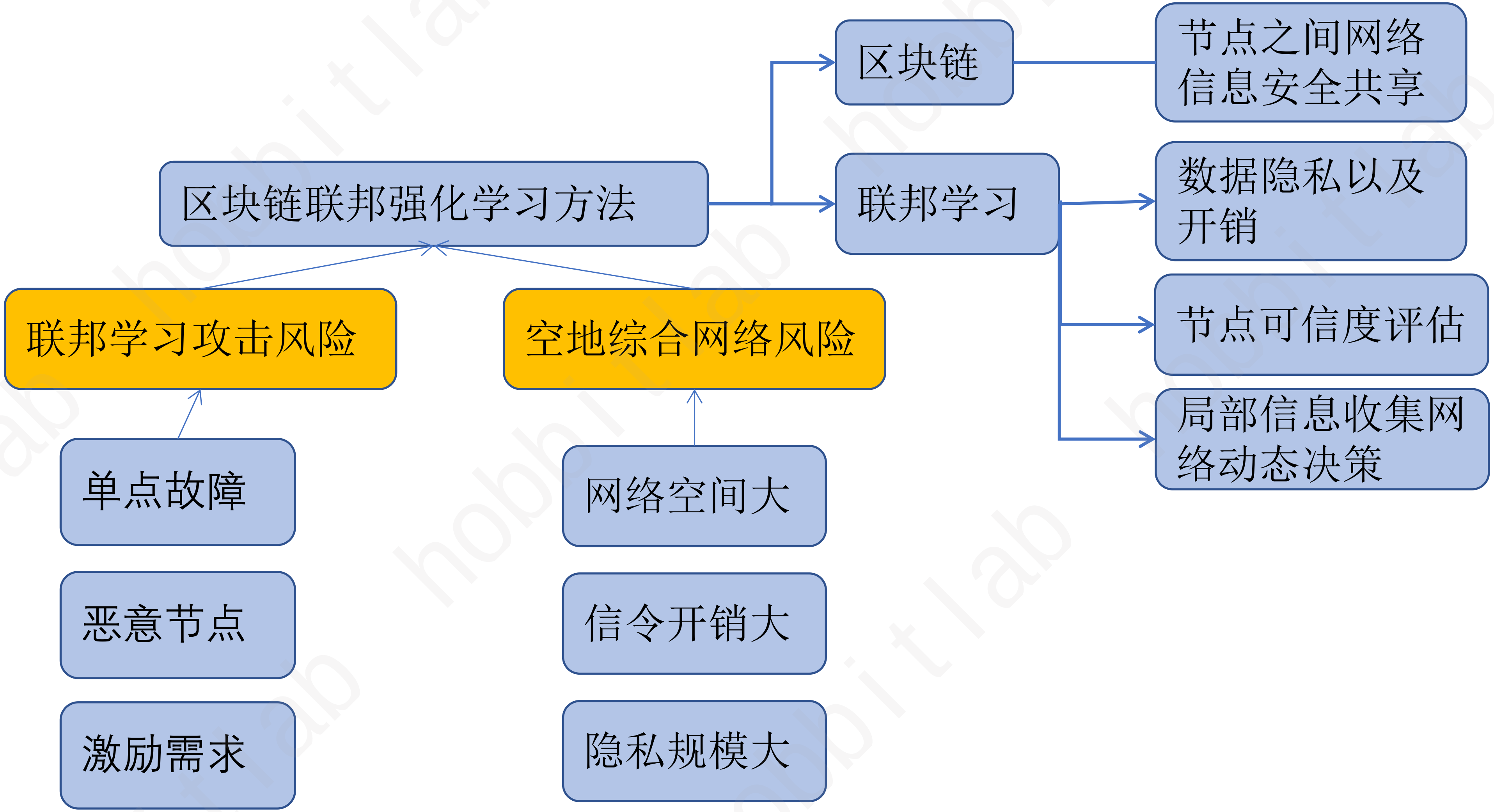
Blockchain-Based Trusted Traffic Offloading in Space-Air-Ground Integrated Networks (SAGIN) A Federated Reinforcement Learning Approach

Huo Mingda

Jinan University, Guangzhou

May 11, 2023

研究内容：


区块链联邦强化学习方法

区块链

节点之间网络信息安全共享

联邦学习

数据隐私以及开销

节点可信度评估

局部信息收集网络动态决策

联邦学习攻击风险

单点故障

恶意节点

激励需求

空地综合网络风险

网络空间大

信令开销大

隐私规模大

研究内容：SAGIN中的卸载解决方案

Huo Mingda, Jinan University

区块链系统

基于区块链的LBS安全保护信任模型

基于节点安全性评价，通过选择机制选择中央共识层的节点

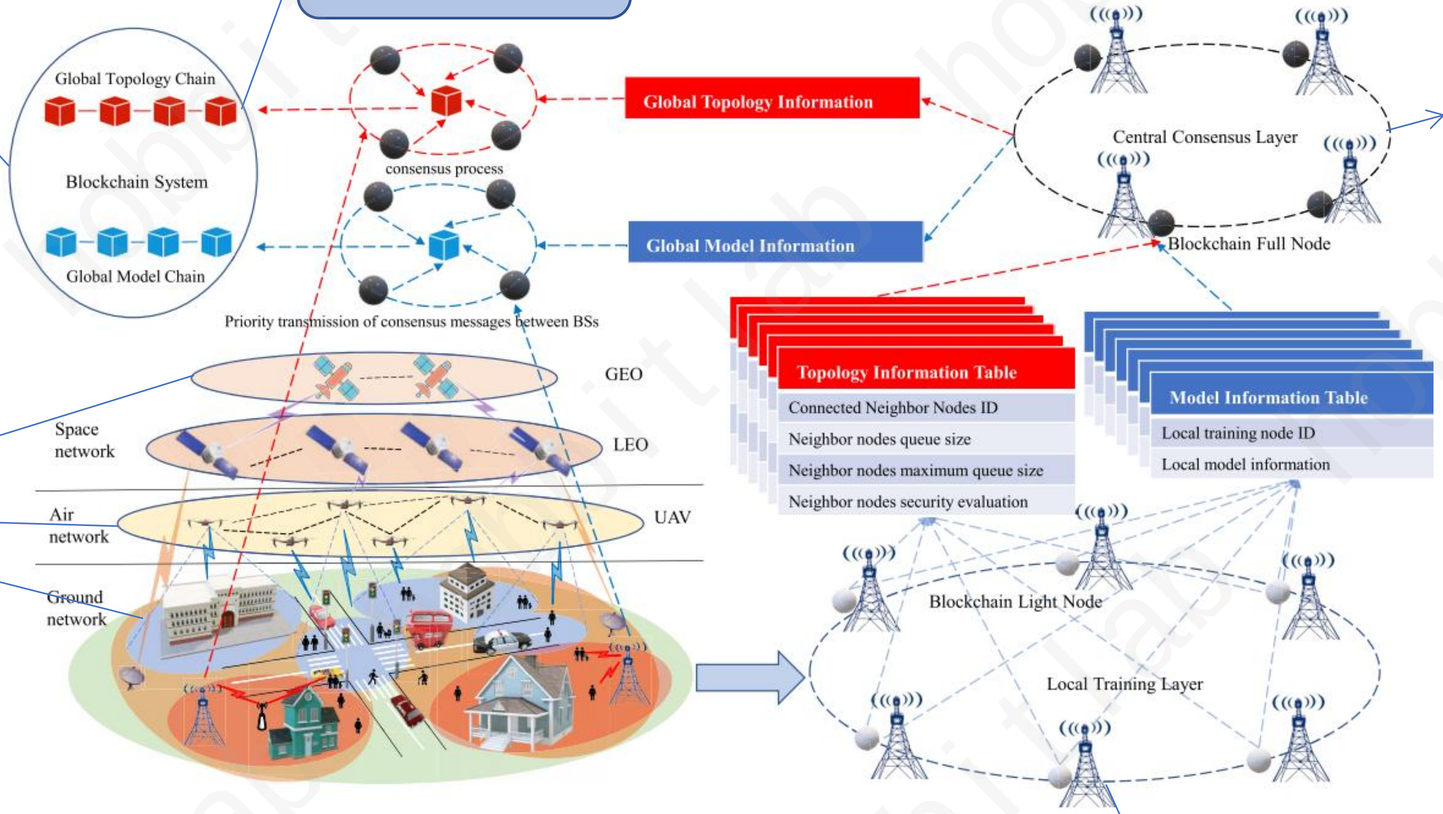
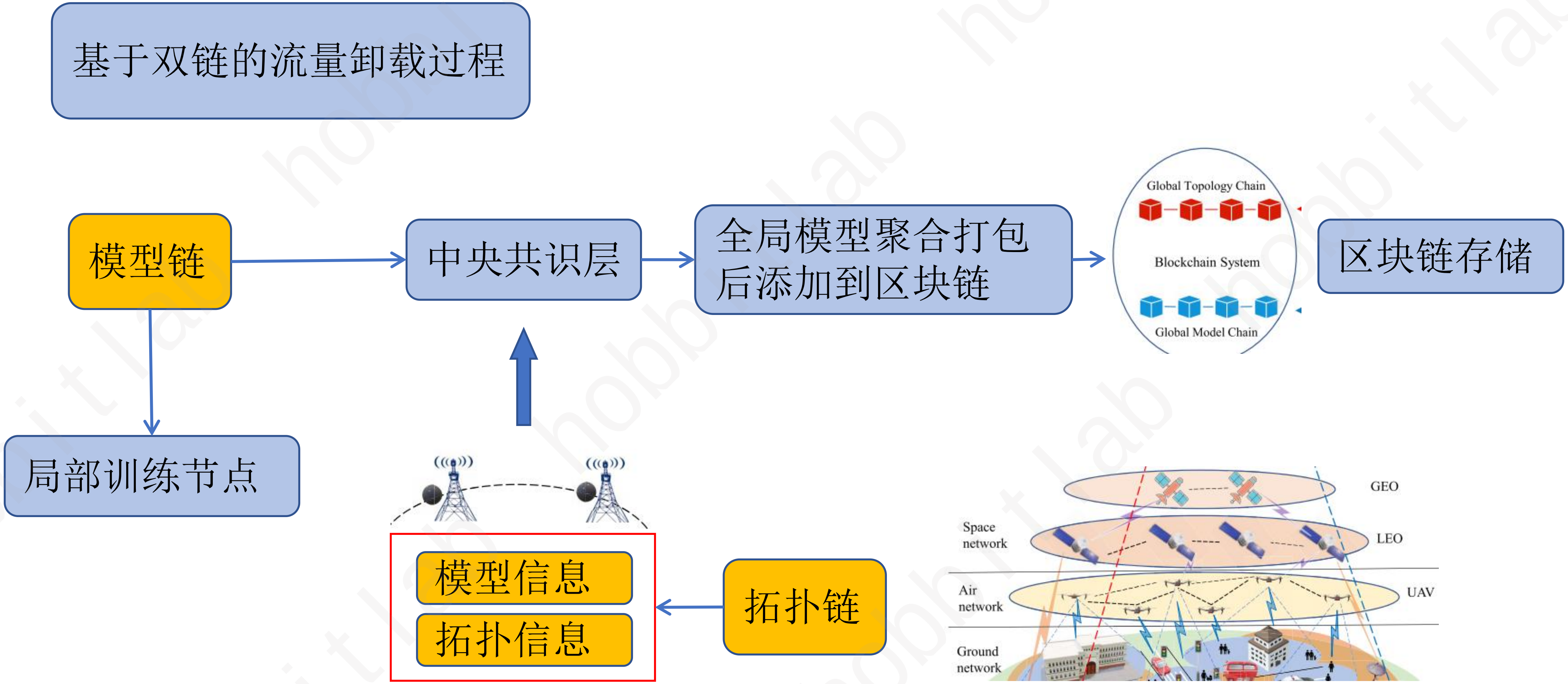


Fig. 1. The architecture of blockchain-based federated learning in SAGIN.

三个网络段

局部训练节点

研究内容：计算卸载策略



基于双链的流量卸载过程

模型链

局部训练节点

中央共识层

全局模型聚合打包后添加到区块链

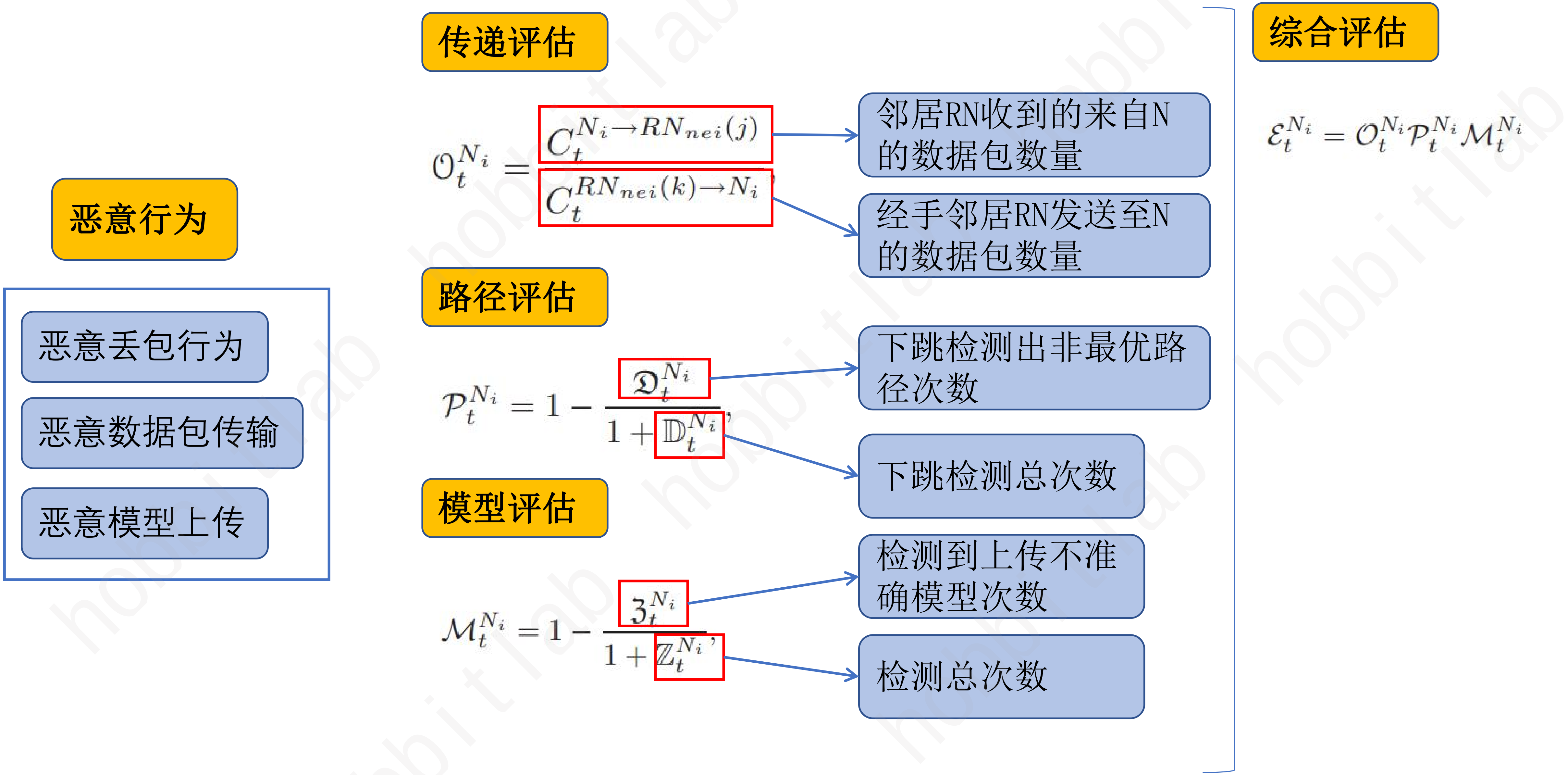
区块链存储

模型信息

拓扑信息

拓扑链

研究内容：节点安全评估机制



恶意行为

- 恶意丢包行为
- 恶意数据包传输
- 恶意模型上传

传递评估

$$\mathcal{O}_t^{N_i} = \frac{\boxed{C_t^{N_i \to RN_{nei}(j)}}}{\boxed{C_t^{RN_{nei}(k) \to N_i}}}$$

邻居RN收到的来自N的数据包数量

经手邻居RN发送至N的数据包数量

路径评估

$$\mathcal{P}_t^{N_i} = 1 - \frac{\boxed{\mathfrak{D}_t^{N_i}}}{1 + \boxed{\mathbb{D}_t^{N_i}}},$$

下跳检测出非最优路径次数

下跳检测总次数

模型评估

$$\mathcal{M}_t^{N_i} = 1 - \frac{\boxed{\mathfrak{Z}_t^{N_i}}}{1 + \boxed{\mathbb{Z}_t^{N_i}},}$$

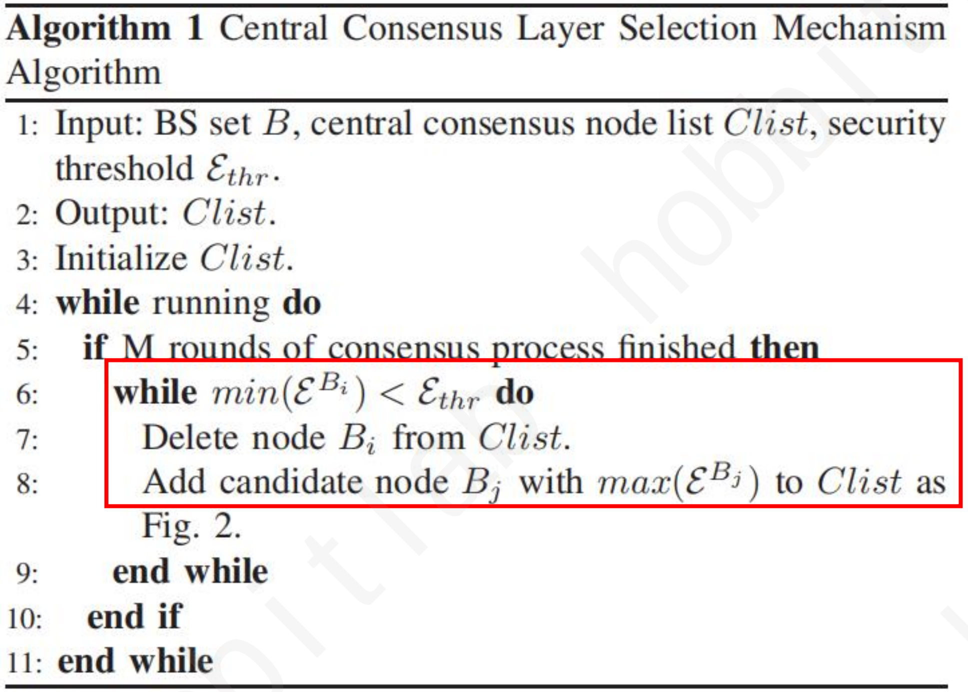
检测到上传不准确模型次数

检测总次数

综合评估

$$\mathcal{E}_t^{N_i} = \mathcal{O}_t^{N_i} \mathcal{P}_t^{N_i} \mathcal{M}_t^{N_i}$$

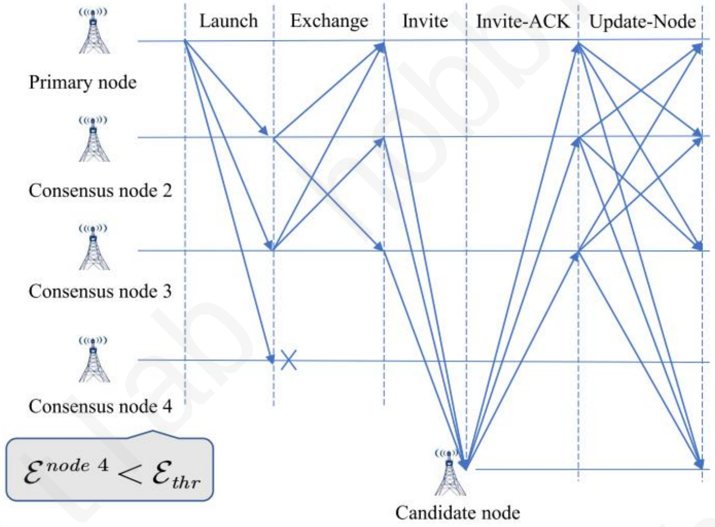
研究内容：共识机制



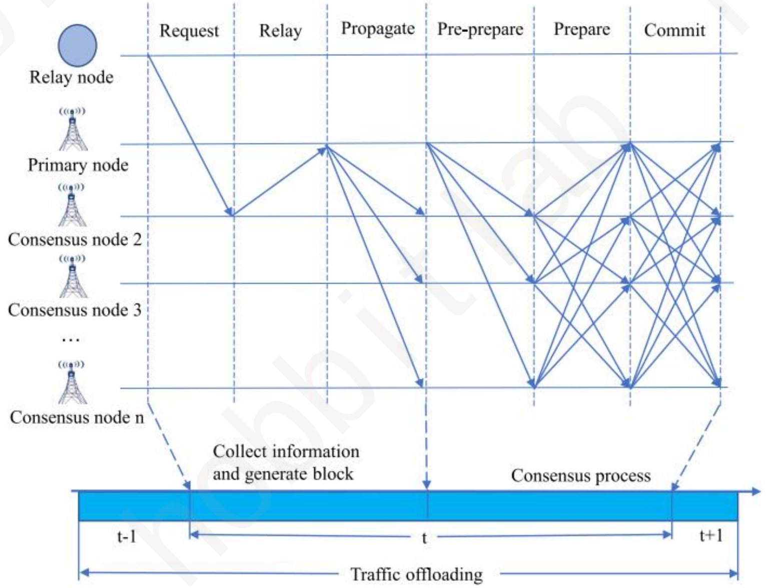
Algorithm 1 Central Consensus Layer Selection Mechanism Algorithm

```
Input: BS set $B$, central consensus node list $Clist$, security threshold $\mathcal{E}_{thr}$.
Output: $Clist$.
Initialize $Clist$.
while running do
    if M rounds of consensus process finished then
        while $min(\mathcal{E}^{B_i}) < \mathcal{E}_{thr}$ do
            Delete node $B_i$ from $Clist$.
            Add candidate node $B_j$ with $max(\mathcal{E}^{B_j})$ to $Clist$ as Fig. 2.
        end while
    end if
end while
```

安全评估值大于安全阈值的BS节点作为中心共识层

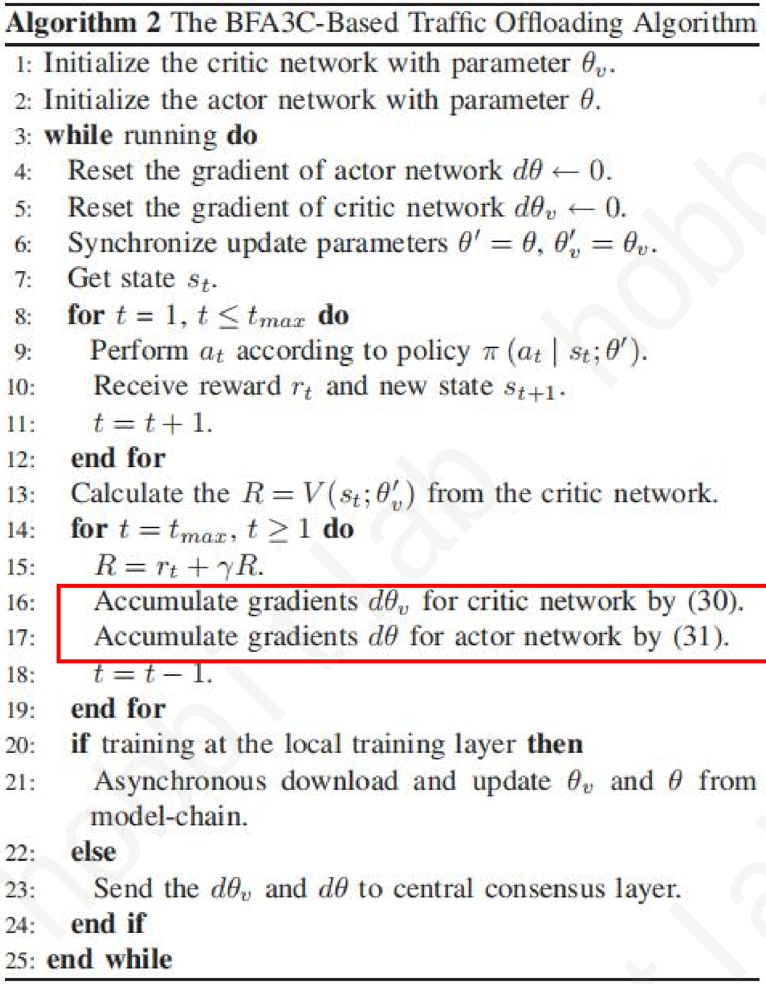


EPBFT的共识节点的更新过程



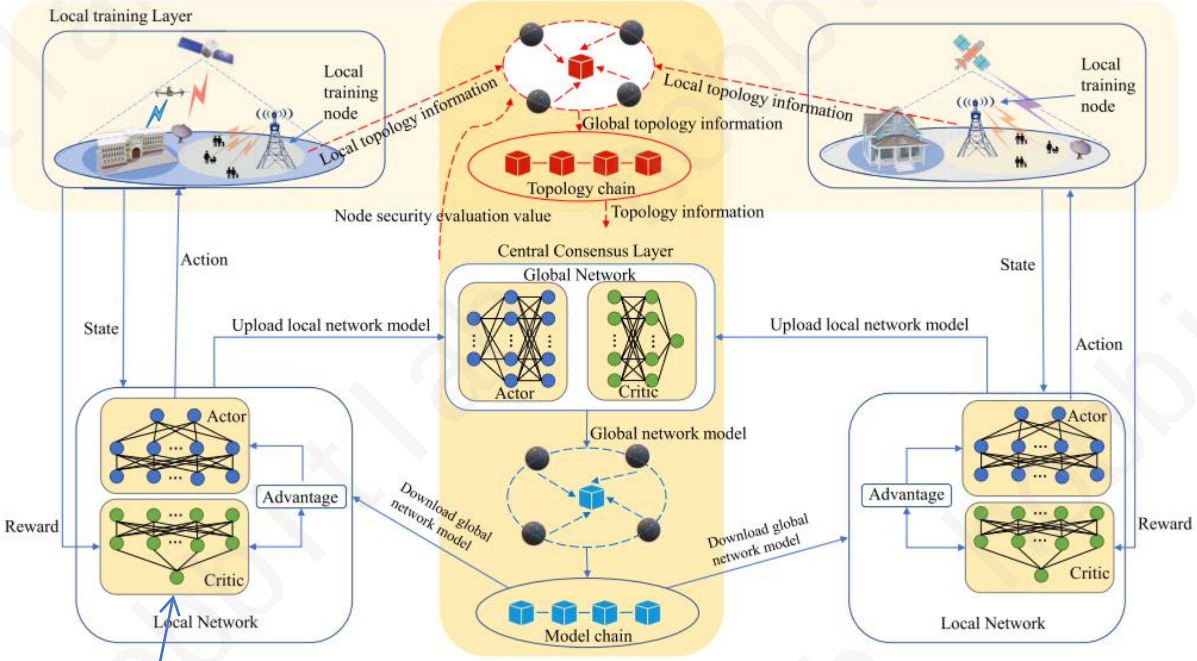
EPBFT的流量卸载和共识过程

研究内容：计算卸载算法



Algorithm 2 The BFA3C-Based Traffic Offloading Algorithm

```
Initialize the critic network with parameter $\theta_v$.
Initialize the actor network with parameter $\theta$.
while running do
    Reset the gradient of actor network $d\theta \leftarrow 0$.
    Reset the gradient of critic network $d\theta_v \leftarrow 0$.
    Synchronize update parameters $\theta' = \theta$, $\theta'_v = \theta_v$.
    Get state $s_t$.
    for $t = 1$, $t \le t_{max}$ do
        Perform $a_t$ according to policy $\pi(a_t \mid s_t; \theta')$.
        Receive reward $r_t$ and new state $s_{t+1}$.
        $t = t + 1$.
    end for
    Calculate the $R = V(s_t; \theta'_v)$ from the critic network.
    for $t = t_{max}$, $t \ge 1$ do
        $R = r_t + \gamma R$.
        Accumulate gradients $d\theta_v$ for critic network by (30).
        Accumulate gradients $d\theta$ for actor network by (31).
        $t = t - 1$.
    end for
    if training at the local training layer then
        Asynchronous download and update $\theta_v$ and $\theta$ from model-chain.
    else
        Send the $d\theta_v$ and $d\theta$ to central consensus layer.
    end if
end while
```



评价网络梯度

参与者网络梯度

仿真实验

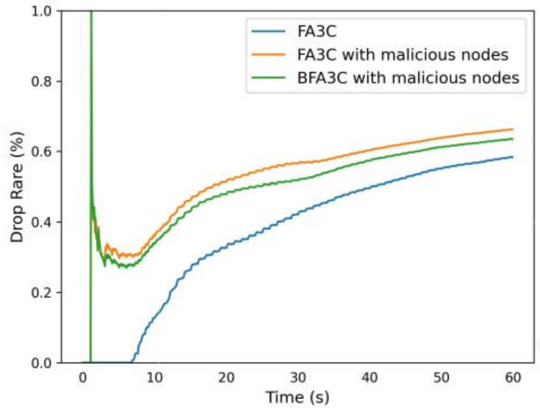


Fig. 5. Packet drop rate over time.

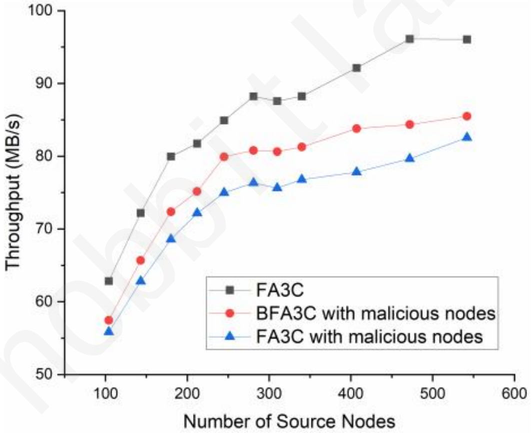


Fig. 7. Throughput per increasing source node count.

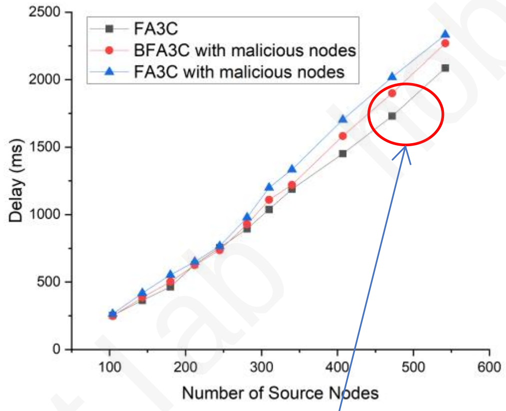


Fig. 9. Packet delay per increasing source node count.

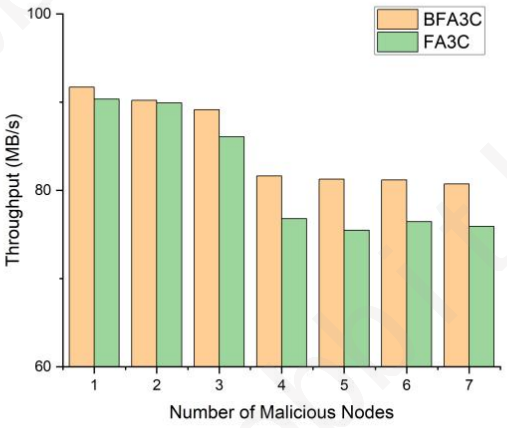


Fig. 11. Throughput per increasing malicious node count.

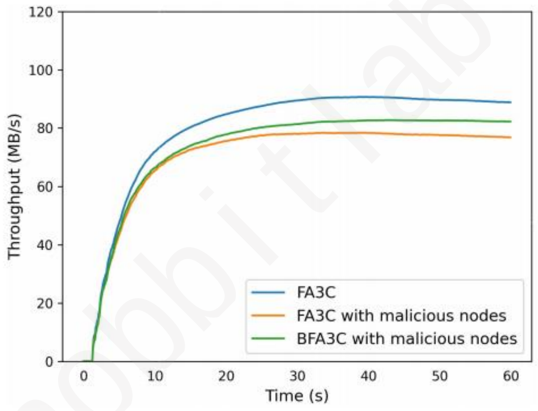
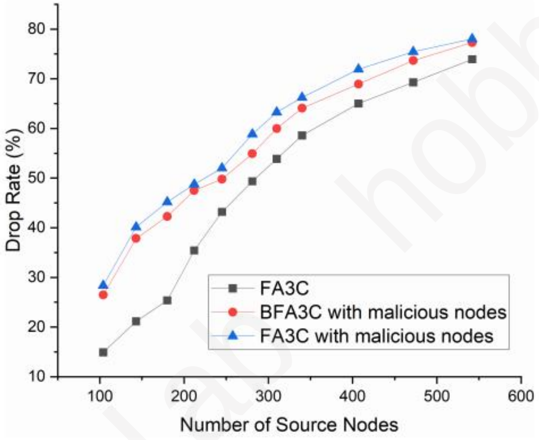


Fig. 6. Network throughput over time.



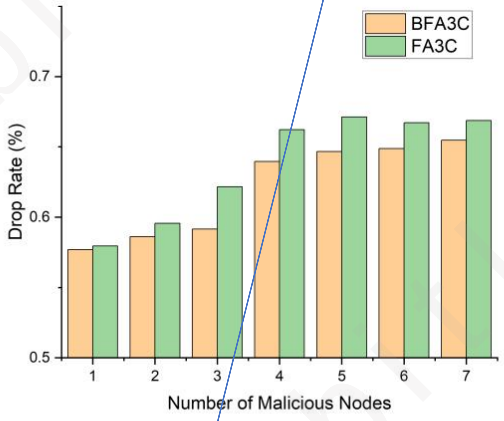


Fig. 10. Drop rate per increasing malicious node count.

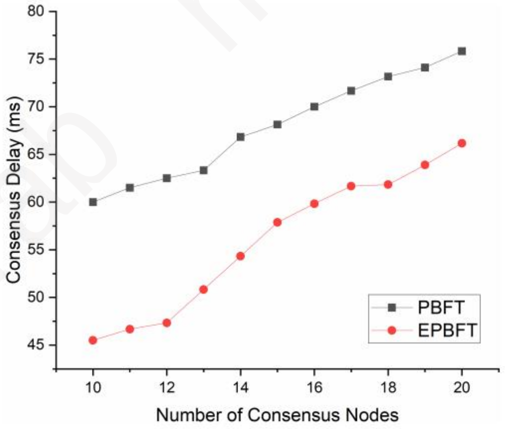


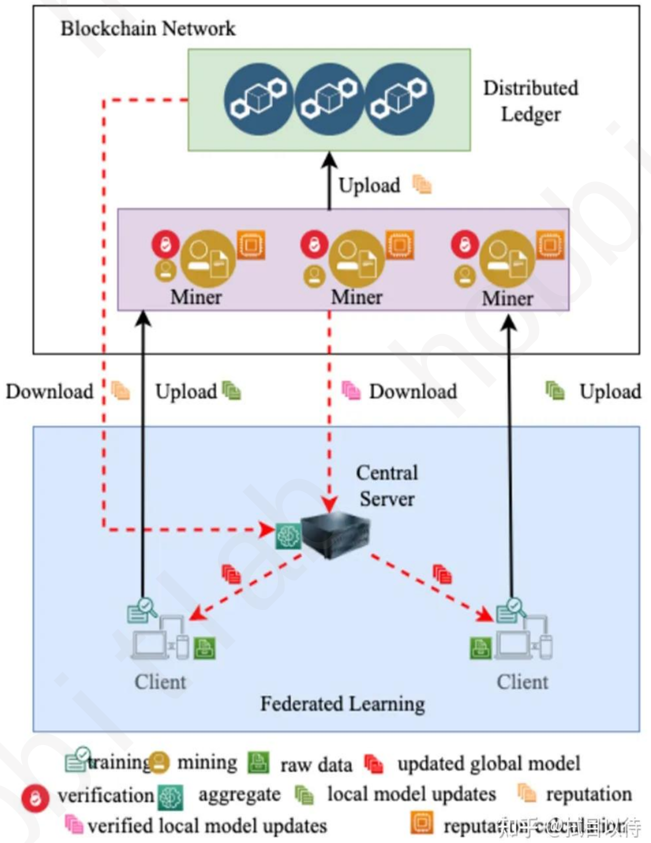
Fig. 12. Consensus delay per increasing consensus node count.

低丢包率，高通信效率

延迟改善

耦合方法总结

联邦学习缺陷	区块链替代了中心化节点
单点故障	验证机制过滤不可信数据
恶意节点	区块链的可审计性
激励需求	分布式存储提高通信效率


Blockchain Network
Distributed Ledger
Upload
Miner
Miner
Miner
Download
Upload
Download
Upload
Central Server
Client
Client
Federated Learning
training
mining
raw data
updated global model
verification
aggregate
local model updates
reputation
verified local model updates
reputation calculation